BIG-IP® Network and System Management Guide

version 9.2.3

MAN-0185-02

Product Version

This manual applies to version 9.2.3 of the BIG-IP® product family.

Publication Date

This manual was published on February 27, 2006.

Legal Notices

Copyright

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

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, Internet Control Architecture, IP Application Switch, iRules, OneConnect, Packet Velocity, SYN Check, Control Your World, ZoneRunner, uRoam, FirePass, TrafficShield, Swan, WANJet, and WebAccelerator are registered trademarks or trademarks, and Ask F5 is a service mark, of F5 Networks, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. F5 Networks' trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Patents

This product protected by U.S. Patents 6,374,300; 6,473,802. Other patents pending.

Export Regulation Notice

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

RF Interference Warning

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

gust 25, 2006.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

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

Canadian Regulatory Compliance

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

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

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

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

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

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

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

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

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

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

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

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

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

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

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

This product includes software developed by Christos Zoulas.

This product includes software developed by 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).

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

Table of Contents

1

Introducing BIG-IP Network and System Management

2

Operating the LCD Panel

3

Lights-Out Management

4

Configuring the BIG-IP Platform and General Properties

5

Configuring VLANs and VLAN Groups

6
Configuring Self IP Addresses

7
Working with Interfaces

8
Configuring Routes

9
Configuring Address Resolution Protocol

10

Working with Trunks

11

Configuring Packet Filters

12

Configuring Spanning Tree Protocols

13
Setting up a Redundant System

14
Managing User Accounts

15
Configuring SNMP

16
Saving and Restoring Configuration Data

17
Logging BIG-IP System Events

18
Configuring BIG-IP System Services

A
Troubleshooting SNMP Traps

B
Configuring bigdb Database Keys

1

Introducing BIG-IP Network and System Management

- Introducing the BIG-IP system
- About this guide
- Finding help and technical support resources

Introducing the BIG-IP system

The BIG-IP® system is a port-based, multilayer switch that supports virtual local area network (VLAN) technology. Because hosts within a VLAN can communicate at the data-link layer (Layer 2), a BIG-IP system reduces the need for routers and IP routing on the network. This in turn reduces equipment costs and boosts overall network performance. At the same time, the BIG-IP system's multilayer capabilities enable the system to process traffic at other OSI layers. The BIG-IP system can perform IP routing at Layer 3, as well as manage TCP, UDP, and other application traffic at Layers 4 through 7. The following modules provide comprehensive traffic management and security for many traffic types. The modules are fully integrated to provide efficient solutions to meet any network, traffic management, and security needs.

- **BIG-IP® Local Traffic Manager**
  The BIG-IP system includes local traffic management features that help make the most of network resources. Using the powerful Configuration utility, you can customize the way that the BIG-IP system processes specific types of protocol and application traffic. By using features such as virtual servers, pools, and profiles, you ensure that traffic passing through the BIG-IP system is processed quickly and efficiently, while meeting all of your security needs. For more information, see the ***Configuration Guide for Local Traffic Management***.

- **BIG-IP® Global Traffic Manager**
  The Global Traffic Manager provide intelligent traffic management to your globally available network resources. Through the Global Traffic Manager, you can select from an array of load balancing modes, ensuring that your clients access the most responsive and robust resources at any given time. In addition, the Global Traffic Manager provides extensive monitoring capabilities so the health of any given resource is always available. For more information, see the ***Configuration Guide for Global Traffic Management***.

- **BIG-IP® Link Controller**
  The Link Controller seamlessly monitors availability and performance of multiple WAN connections to intelligently manage bi-directional traffic flows to a site - providing fault tolerant, optimized Internet access regardless of connection type or provider. The Link Controller ensures that traffic is always sent over the best available link to maximize user performance and minimize bandwidth cost to a data center. For more information, see the ***Configuration Guide for the BIG-IP Link Controller***.

- **BIG-IP®Application Security Module**
  The Application Security Module provides web application protection from application-layer attacks. The Application Security Module protects Web applications from both generalized and targeted application layer attacks including buffer overflow, SQL injection, cross-site scripting, and parameter tampering. For more information, see the ***Configuration Guide for the BIG-IP Application Security Module***.

Overview of BIG-IP network management features

In a typical configuration, the BIG-IP system functions as a device on the network, directing different types of protocol and application traffic to an appropriate destination server. The system accomplishes this by either forwarding the traffic directly to a load balancing server pool, or by sending it to a next-hop router or a pool of routers. The most basic configuration of the BIG-IP system includes two virtual local area networks (VLANs) with one or more BIG-IP system interfaces (ports) assigned to each VLAN. Using the BIG-IP system's browser-based Configuration utility, you can assign multiple interfaces to each VLAN, or you can configure the BIG-IP system to send traffic for multiple VLANs through the same interface.

The BIG-IP system consists of several fundamental network components that you can configure in the way that best utilizes BIG-IP system capabilities.

Interfaces, spanning tree protocols, and trunks

A BIG-IP system has several interfaces for switching or routing traffic from various hosts or other devices on the network. ***Interfaces*** are the hardware ports that the BIG-IP system uses to send and receive traffic. When you create a virtual local area network (VLAN) on the BIG-IP system, you can assign multiple interfaces to that VLAN. You can also assign the same interface to multiple VLANs. For more information, see Chapter 7, *Working with Interfaces*.

When you connect multiple switches to the BIG-IP system in parallel, you can configure your hosts to make use of spanning tree protocols. ***Spanning tree protocols*** provide path redundancy while preventing unwanted loops in the network. You can view spanning tree instances, configure global spanning tree options, and configure spanning tree settings for each interface. For optimal performance, you can use spanning tree protocols in conjunction with the trunks feature. For more information, see Chapter 12, *Configuring Spanning Tree Protocols*.

Trunks are a feature you can use to aggregate your links. When you create ***trunks,*** you group interfaces together to function as one larger interface and to provide redundancy if one interface in the trunk becomes unavailable. When that occurs, traffic can be processed on another interface in the trunk. For more information, see Chapter 10, *Working with Trunks*.

VLANs and self IP addresses

A virtual local area network, or ***VLAN***, is a logical collection of hosts on the network. Each VLAN has one or more BIG-IP system interfaces associated with it. VLANs have these primary advantages:

- **VLANs define boundaries for a broadcast domains**.
  Traditionally, network administrators have deployed routers within the same IP network, to define smaller broadcast boundaries. A better solution is to use VLANs. When a host in a VLAN sends a broadcast message to find the MAC address of a destination host, the message is sent to only those hosts in the VLAN. Using VLANs to control the boundaries of broadcast domains prevents messages from flooding the network, thus enhancing network performance.
- **VLANs ease system and network maintenance**
  Normally, the way to enable hosts to share network resources, such as storage devices and printers, has been to group hosts into the same physical location. Continually moving and re-cabling hosts to other locations on the network, as well as manually updating routing tables, can be a costly and time-consuming task for a system or network administrator. Using VLANs, you can avoid these problems. All hosts that you group within a VLAN can share network resources, regardless of their physical location on the network.

To enhance performance and flexibility, the BIG-IP system comes with two existing virtual local area networks (VLANs), one for your external network, and one for your internal network. Each of these VLANs has a BIG-IP system interface already assigned to it. You can use these two VLANs as is, you can assign additional interfaces to these VLANs, or you can create more VLANs. A key feature of the BIG-IP system is that a single interface can forward traffic for multiple VLANs. For more information, see Chapter 5, *Configuring VLANs and VLAN Groups*.

Each VLAN you create has its own ***self IP address***. The BIG-IP system uses this address as the source IP address when sending requests to hosts in a VLAN, and hosts in a VLAN use this IP address as the destination IP address when sending responses to the BIG-IP system.

When you first ran the Setup utility, you assigned a self IP address to the internal VLAN, and another self IP address to the external VLAN. As you create other VLANs, you assign self IP addresses to them, too. Also, units of a redundant system can share a self IP address, to ensure that the BIG-IP system can process server responses successfully when failover has occurred. For more information, see Chapter 6, *Configuring Self IP Addresses*.

IP routing and ARP

Another feature that should be familiar to network administrators for managing the BIG-IP system's Layer 3 functions is the routing table. Using the ***routes*** feature, you can explicitly add routes that you want the BIG-IP system to use when functioning as a layer 3 device to forward packets around the network, or you can view the dynamic routes that the BIG-IP system automatically adds to its routing table.

The Address Resolution Protocol, or ***ARP***, feature gives you the ability to view or add entries to the ARP cache, which the BIG-IP system uses to match IP addresses to Media Access Control (MAC) addresses when using layer 3 to send packets to destination hosts. When you want to eliminate the need to use IP routing to send ARP requests from one VLAN to another, you can enable the proxy ARP feature. A host configured with the ***proxy ARP*** feature can send ARP requests to another VLAN using layer 2 forwarding instead of IP routing. For more information, see Chapter 9, *Configuring Address Resolution Protocol*.

Packet filtering

A powerful security feature that the BIG-IP system offers is packet filtering. Using ***packet filtering***, you can control and restrict the types of traffic passing through the BIG-IP system. Besides defining the action that the BIG-IP system should take when receiving a packet (accept, discard, or reject), you can exempt certain types of traffic from packet filtering, based on protocol, IP address, MAC address, or VLAN. For more information, see Chapter 11, *Configuring Packet Filters*.

Overview of BIG-IP system management features

This guide addresses some of the system management options that are common to all BIG-IP systems. These options include creating and maintaining administrative user accounts, configuring System Network Management Protocol (SNMP), and configuring and maintaining redundant systems.

You partially configure some of these options by running the Setup utility on the BIG-IP system. Once you have run the Setup utility, you can use the Configuration utility to complete the configuration of these options and to manage the BIG-IP system on an ongoing basis.

Liquid crystal display and lights-out management

Using the ***liquid crystal display (LCD)***, you can control the BIG-IP unit without attaching a serial or network cable.With the ***lights out management*** feature, you can remotely manage certain aspects of the operation of the hardware unit and the BIG-IP traffic management operating system in the event that the traffic management software becomes incapacitated. For more information, see Chapter 2, *Operating the LCD Panel*, and Chapter 3, *Lights-Out Management*.

User accounts and user roles

You can create or manage user accounts for BIG-IP system administrators. These accounts can reside either locally on the BIG-IP system, or remotely on a separate authentication server such as a Lightweight Directory Access Protocol (LDAP) server. You can also manage the three special user accounts **root**, **admin**, and **support**.

For each new user account that you create, you can assign a user role that defines the type and level of access granted to that user. The available user roles are: **Administrator**, **Operator**, **Guest**, and **No Access**.

The types of remote authentication servers that you can use to store user accounts for BIG-IP system administrators are: Active Directory™ servers, Lightweight Directory Access Protocol (LDAP) servers, and Remote Authentication Dial-in User Service (RADIUS) servers. For more information, see Chapter 14, *Managing User Accounts*.

System Network Management Protocol (SNMP)

System Network Management Protocol (SNMP) is an industry-standard protocol that allows you to manage the BIG-IP system remotely, along with other devices on the network. The BIG-IP system provides the SNMP agent and the MIB files that you need to manage the system remotely using SNMP. For more information, see Chapter 15, *Configuring SNMP*.

Redundant systems

To ensure high-availability of the BIG-IP system, you can set up a redundant-system configuration. Then, if one BIG-IP system becomes unavailable, another BIG-IP system can immediately take over to process the traffic.

When you first run the Setup utility on a BIG-IP system, you specify whether the system is a unit of a redundant pair. When you configure two BIG-IP systems to function as units of a redundant system, a process known as failover occurs when one of those units becomes unavailable for any reason. ***Failover*** ensures that the BIG-IP system can still process traffic when a unit is unavailable.

Every redundant system has a mode that you specify, either active/standby or active-active. If you choose active/standby mode and failover occurs later, then by default the standby unit becomes active, and remains active, until failover occurs again. If you choose active-active mode, the surviving unit begins processing connections targeted for the failed unit, while continuing to process its own connections. In this way, users experience no interruption in service in the event of system unavailability. For more information, see Chapter 13, *Setting up a Redundant System*.

Logging

Using the **Syslog-ng** utility, the BIG-IP system logs many different types of events, related to the operating system, packet filtering, local traffic management, and auditing. You can use the Configuration utility to display each type of event. For specific types of local traffic events, because each individual event is associated with a severity, you can set a minimum log level on an event type. Setting a minimum log level on an event type affects which messages the system displays, based on event severity. For example, you can set a minimum log level of **Warning** on ARP-related events, which then causes the system to display only those ARP-related events that have a severity of **Warning** or higher (that is, more severe). For more information, see Chapter 17, *Logging BIG-IP System Events*.

BIG-IP system services

The BIG-IP system includes several different services. Some of these services, such as MCPD and TMM, must be running in order to process application traffic, while others are optional, such as **postfix** or **radvd**.

A core set of services have heartbeats and are associated with failover in a redundant system. When you configure a redundant system, you can specify the action that you want the BIG-IP system to take if it fails to detect a heartbeat. For example, you can configure the BIG-IP system to reboot if it fails to detect a heartbeat for the MCPD service. Finally, there are times when you might need to stop a service in order to perform a specify system-management task. For example, we recommend that you stop the TMM service when installing a new version of the BIG-IP system. For more information, see Chapter 18, *Configuring BIG-IP System Services*.

Archives

Every BIG-IP system includes a set of essential configuration data that you create when you initially configure your system. To protect this data in the event of a system problem, you can create an archive, also known as a**.ucs** file. An archive is a backup copy of your configuration data that you create and store on the BIG-IP system. If your original configuration data becomes corrupted for some reason, you can use the archive to restore the data. As an added layer of protection, you can download your archives to a remote system, in case the BIG-IP system itself becomes unavailable. When the system is up and running again, you can upload the data back onto the system. For more information, see Chapter 16, *Saving and Restoring Configuration Data*.

Choosing a configuration tool

The BIG-IP system offers a browser-based utility for managing the BIG-IP system, and, as an alternative, various command line utilities. Note that all procedures in this guide describe how to manage the system using the browser-based utility.

The Configuration utility

The Configuration utility is a browser-based application that you use to configure and monitor the BIG-IP system. Once you complete the instructions for the Setup utility, you can use the Configuration utility to perform additional configuration steps necessary for your chosen load balancing solution. In the Configuration utility, you can also monitor current system performance, and download administrative tools such as the SNMP MIBs or the SSH client. The Configuration utility requires Netscape Navigator version 4.7, or Microsoft Internet Explorer version 5.0 or 5.5.

One of the tasks you can perform with the Configuration utility is setting user preferences. Setting user preferences customizes the way that the Configuration utility displays information for you. For example, when you display a list of objects such as the virtual servers that you have created, the utility normally displays ten objects, or records, per screen. However, you can change this value so that the utility displays more, or fewer, than ten records per screen.

Table 1.1 lists and describes the preferences that you can configure to customize the display of the Configuration utility. Following this table is the procedure for configuring these preferences..

Setting	Description	Default Value
Records per Screen	Specifies, for all list screens, the number of records that the system displays by default. The default setting is **10**.	**10**
Start Screen	Specifies the screen that displays when you open a new browser session for this system. Possible values are: **Welcome**, **Traffic Summary**, **Performance**, **Statistics**, and **Virtual Servers**.	**Welcome**
Advanced by Default	Specifies, when checked, that the system expands the configuration options from **Basic** to **Advanced**. The **Basic** setting displays the most common and more frequently-edited settings for a feature, while the **Advanced** setting displays all of the settings for a feature. ***Note:*** *This is a display feature only; when you select* ***Basic****, any options that remain hidden still apply to the configuration, with their default values.*	**Advanced**
Display Host Names When Possible	Specifies, when checked, that the system displays host names, rather than IP addresses, if the IP address has host name associated with it.	Disabled (unchecked)
Statistics Format	Specifies the format for the statistical data. Select **Normalized** if you want the system to display rounded values. Select **Unformatted** if you want the system to display the actual values to all places. Note that you can override the default format on the individual statistics screens.	**Normalized**

Table 1.1 *Configuration utility preferences*

Setting	Description	Default Value
Default Statistics Refresh	Specifies the default rate at which the system refreshes statistical data. Possible values are: **10 seconds**, **20 seconds**, **30 seconds**, **60 seconds**, **3 minutes**, and **5 minutes**. Note that you can override the default refresh rate on the individual statistics screens.	**Disabled**
Archive Encryption	Specifies whether the BIG-IP encrypts all archives (**.ucs** files) that you create. Possible values are: **On Request** -- Causes the encryption of archives to be optional. **On** -- Causes the BIG-IP system to automatically encrypt all archives that you create. When you select this value, you must create a passphrase when you create an archive. **Off** -- Prevents you from encrypting any archive that you create. When you select this value, the **Encryption** setting on the New Archive screen becomes unavailable.	**On Request**

Table 1.1 *Configuration utility preferences*

To configure user preferences

1. On the Main tab of the navigation pane, expand **System**, and click **Preferences**.
   The Preferences screen opens.
2. Configure each preference or retain the default value.
3. Click **Update**.

Command-line utilities

In addition to using the Configuration utility, you can also manage the BIG-IP system using command-line utilities such as the **bigpipe** utility™. To monitor the BIG-IP system, you can use certain **bigpipe** commands, or you can use the **bigtop**™ utility, which provides real-time system monitoring. You can use the command line utilities directly on the BIG-IP system console, or you can run commands using a remote shell, such as the SSH client or a Telnet client. For more information on command-line utilities, see the online man pages.

About this guide

Before you use this guide, we recommend that you run the Setup utility on the BIG-IP system to configure basic network and network elements such as static and floating self IP addresses, interfaces, and VLANs, to name a few.

After running the Setup utility, you can further customize your system by using the Configuration utility to create local traffic management objects such as virtual servers, load balancing pools, and profiles.

Finally, you can return to this guide to adjust the elements you have configured, or to add additional ones as your needs change.

Before you continue with adjusting or customizing your BIG-IP system configuration, complete these tasks:

- Choose a configuration tool.
- Familiarize yourself with additional resources such as product guides and online help.
- Review the stylistic conventions that appear in this chapter.

Additional information

In addition to this guide, there are other sources of the documentation you can use in order to work with the BIG-IP system. The information is organized into the guides and documents described below. The following printed documentation is included with the BIG-IP system.

- **Configuration Worksheet**
  This worksheet provides you with a place to plan the basic configuration for the BIG-IP system.
- **BIG-IP Quick Start Instructions**
  This pamphlet provides you with the basic configuration steps required to get the BIG-IP system up and running in the network.

The following guides are available in PDF format from the CD-ROM provided with the BIG-IP system. These guides are also available from the first Web page you see when you log in to the administrative web server on the BIG-IP system.

- **Platform Guide**
  This guide includes information about the BIG-IP system. It also contains important environmental warnings.
- **Installation, Licensing, and Upgrades for BIG-IP Systems**
  This guide provides detailed information about installing upgrades to the BIG-IP system. It also provides information about licensing the BIG-IP system software and connecting the system to a management workstation or network.
- **Configuration Guide for Local Traffic Management**
  This guide contains any information you need for configuring the BIG-IP system to manage local network traffic. With this guide, you can perform

tasks such as creating virtual servers and load balancing pools, configuring application and persistence profiles, implementing health monitors, and setting up remote authentication.

Stylistic conventions

To help you easily identify and understand important information, all of our documentation uses the stylistic conventions described here.

Using the solution examples

All examples in this document use only private class IP addresses. When you set up the solutions we describe, you must use valid IP addresses suitable to your own network in place of our sample addresses.

Identifying new terms

To help you identify sections where a term is defined, the term itself is shown in bold italic text. For example, a ***floating IP address*** is an IP address assigned to a VLAN and shared between two computer systems.

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, with the **bigpipe self <ip_address> show** command, you can specify a specific self IP address to show by specifying an IP address for the **<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 SNMP traps in Appendix *A, Troubleshooting SNMP Traps.*

Identifying command syntax

We show 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 shows the configuration of the specified pool name:

```
bigpipe self <ip_address> show
```

or

```
b self <ip_Address> show
```

Table 1.2 explains additional special conventions used in command line syntax.

Item in text	Description
\	Indicates that the command continues on the following line, and that users should type the entire command without typing a line break.
< >	Identifies a user-defined parameter. For example, if the command has **<your name>**, type in your name, but do not include the brackets.
|	Separates parts of a command.
[]	Indicates that syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

Table 1.2 *Command line syntax conventions*

Finding help and technical support resources

You can find additional technical documentation and product information in the following locations:

- **Online help for local traffic management**
  The Configuration utility has online help for each screen. The online help contains descriptions of each control and setting on the screen. Click the Help tab in the left navigation pane to view the online help for a screen.

- **Welcome screen in the Configuration utility**
  The Welcome screen in the Configuration utility contains links to many useful web sites and resources, including:

  - The F5 Networks Technical Support web site
  - The F5 Solution Center
  - The F5 DevCentral web site
  - Plug-ins, SNMP MIBs, and SSH clients

- **F5 Networks Technical Support web site**
  The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest documentation for the product, including:

  - Release notes for the the BIG-IP system, current and past
  - Updates for guides (in PDF form)
  - Technical notes
  - Answers to frequently asked questions
  - The Ask F5 natural language question and answer engine.

  To access this site, you need to register at **http://tech.f5.com**.

2

Operating the LCD Panel

- Introducing the LCD panel
- Using the LCD panel
- Navigating through the LCD menus

Introducing the LCD panel

The liquid crystal display, or LCD panel, provides the ability to control the unit without attaching a serial or network cable. The following menus are available on the LCD panel.

- **Information menu**
  Use the Information menu to find information about using the LCD and its functionality.
- **System menu**
  Use the System menu to reboot, notebook, or halt the unit. This menu also has options for setting the properties of the management interface (MGMT) and the serial port.
- **Screen menu**
  Use the Screen menu to set up the informational screens you would like the LCD to cycle through. The information screens include system status, statistics, and system alerts.
- **Options menu**
  Use the Options menu to configure the properties of the LCD panel.

This chapter describes how to use the LCD panel and its menus. It does not describe each function available in each menu.

Figure 2.1 shows an example of the LCD panel and control buttons.

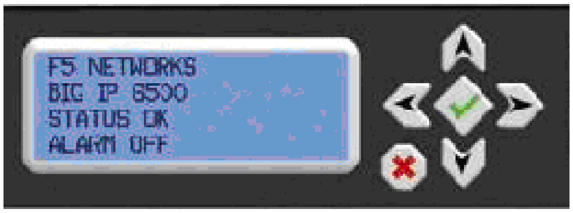


Figure 2.1 *An example of the LCD panel and control buttons*

Using the LCD panel

You can configure the LCD panel to meet your needs. The following section describes how to perform a number of tasks with the LCD panel:

- Pause on a screen
- Use the LCD menus
- Power up the unit
- Halt the unit
- Power down the unit
- Reboot the unit

Pausing on a screen

Normally, the screens cycle on the LCD at a constant rate. However, push the Check button to toggle the LCD between Hold and Rotate modes. In Hold mode, a single screen is displayed. The Rotate mode changes the screen displayed on the LCD every 4 seconds.

Using LCD menus

Pressing the **X** button puts the LCD panel in Menu mode. The buttons Left Arrow, Right Arrow, Up Arrow, and Down Arrow are only functional when the LCD is in Menu mode.

Powering up the unit

When you want to power on a unit that is shut down, press the Check button to turn the power on.

Halting the unit

We recommend you halt the unit before you power it down or reboot it using the LCD menu options.

To halt the unit

1. Press the **X** button, then use the arrow keys to navigate to the System menu.
2. Press Check. Navigate to the Halt menu.
3. Press the Check button. Press the Check button again at the confirmation screen.
4. Wait 50 seconds before powering the machine off or rebooting it.

Powering down the unit

Hold the **X** button for 4 seconds to power down the unit. We recommend that you halt the system before you power down the system in this manner.

Rebooting the unit

Hold the Check button for 4 seconds to reboot the unit. You should only use this option after you halt the unit.

Clearing alerts

Press the Check button to clear any alerts on the LCD screen. You must clear any alerts on the screen before you can use the LCD.

Navigating through the LCD menus

To use the LCD menus, you must first put the LCD in menu mode. To put the LCD in menu mode, press the **X** button.

After you put the LCD in menu mode, use the Left Arrow, Right Arrow, Up Arrow, and Down Arrow buttons to select menu options. There are four menu options:

- Information
- System
- Screens
- Options

The following tables describe each LCD menu option.

Information menu

You can use the Information menu to access help pages about using the LCD panel functionality. You can also find more information on what different LED activity means, and the failover state of the unit in a redundant pair. The following table, Table 2.1, shows the options available on the Information menu.

Option	Description
How to use the LCD	Displays a vertical scrolling text description on how to use the LCD panel.
Front Panel LEDs	Displays a vertical scrolling text description of what the front panel LEDs mean.
Port Indicators	Displays a vertical scrolling text description of what the lights above the ports mean.
Console and Failover serial port information	Displays a vertical scrolling text description of the console and failover serial ports.

Table 2.1 *The Information menu*

System menu

The System menu provides various options for rebooting, halting, or netbooting the hardware. This menu also provides options for configuring the network on the management interface. The following table, Table 2.2, lists the options available in the System menu.

Option	Description
Reboot	Select this option to reboot the unit.
Halt	Select this option to halt the unit.
Netboot	Select this option if you are installing software from a PXE server.
IP address	Type the management interface IP address. You can only use an IPv4 address.
Netmask	Set the netmask for the management interface IP address.
Default route	Type in the default route for the management interface. This route is necessary if you plan to manage the unit from a different subnetwork.
Commit	Select this option to commit your changes.
Serial port	Use this option to change the baud rate of the serial port. The following options are available: 9600 19200 38400 115200

Table 2.2 *The System menu*

Screens menu

You can use the Screens menu options to view various statistics and information about the system. The following table, Table 2.3, lists all the general information screens. You can use the LCD button to place a check mark next to the name of the screens you would like to appear when the screens cycle.

Option	Description
Version screen	Displays the product version information.
Information screen	Displays the information screen menu.
Date and Time screen	Displays the date and time.
MAC addresses screen	Displays the MAC addresses on the unit.

Table 2.3 *The general screen information menu*

Option	Description
System information screen	Displays system information.
CPU usage	Displays the CPU usage percentage.
Memory usage	Displays the memory usage.
Auth requests	Displays the number of authentication requests being processed.
Statistics	Displays simple statistics, such as bytes and packets in and out of the system.
Alert screen	Displays system alerts.

Table 2.3 *The general screen information menu*

Options menu

You can use the Options menu to adjust the display properties of the LCD panel. The following table, Table 2.4, lists the options available on the Options menu.

Option	Description
Contrast	Use the Left and Right arrow keys on the LCD to set the contrast of the LCD.
On Brightness	This setting provides the ability to adjust the LCD backlight brightness.
Off Brightness	This setting controls the brightness of the LCD panel when the backlight is off. Use the Left and Right arrow keys to set the brightness of the LCD panel.

Table 2.4 *The Options menu*

3

Lights-Out Management

Introducing lights-out management

A lights-out management system is available with the latest F5 Networks platforms. The ***lights-out*** management system provides the ability to remotely manage certain aspects of the operation of the hardware unit and the BIG-IP traffic management operating system in the event the traffic management software becomes incapacitated.

The lights-out management system consists of the following elements.

- **Switch card control processor (SCCP)**
  The hardware that provides the hardware control over the whole unit.
- **Host console shell (hostconsh)**
  The shell that provides access to the command menu.
- **Command menu**
  The menu that contains the options for lights-out management.
- **Traffic management operating system**
  The software that you configure to manage the traffic for your site.
- **Out-of-band management commands**
  The commands that provide the ability to control various aspects of the system with a series of keystrokes.

The command menu operates independently of the traffic management operating system through the management port, the serial port console, and remotely through the traffic management ports.

- You can use the command menu to reset the unit, even if the BIG-IP traffic management system has locked up.
- You can remotely set a unit to netboot for a software re-install from an ISO image.
- You can get console access to the BIG-IP traffic management system itself, so you can configure the traffic management system from the command line interface.

The lights-out management system and the BIG-IP traffic management system function independently within the hardware unit. Figure 3.1 shows the relationship between the lights-out management system and the traffic management system.

The lights-out management system is accessible through the management interface (number 1 in Figure 3.1) and the console port (number 2 in Figure 3.1). This functionality is independent of the traffic management system (number 3 in Figure 3.1).

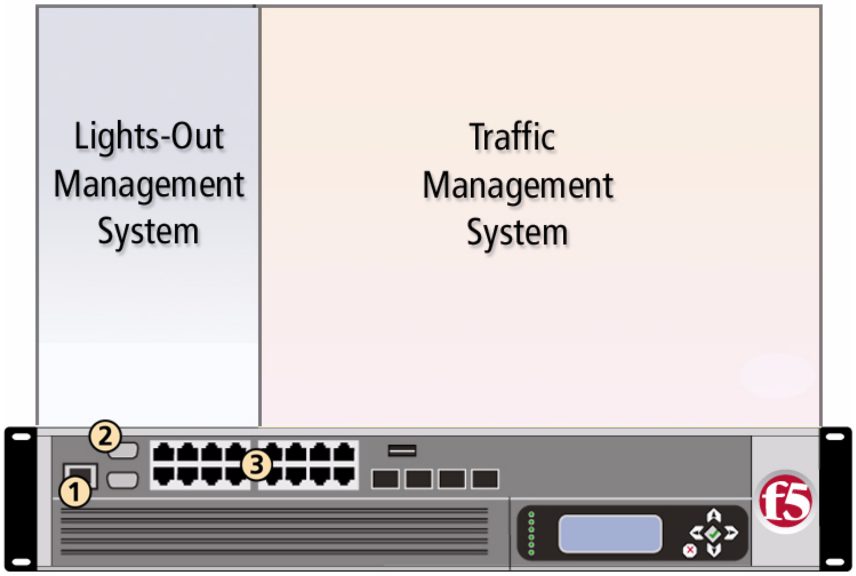


Figure 3.1 *The lights-out management system and the traffic management system.*

Accessing the command menu

You can access the command menu through the host console shell (**hostconsh**) using the front panel serial console, or remotely through SSH. The following section describes how to access the command menu both through the serial console and with an SSH client to the management interface.

Options for accessing the command menu

There are two methods you can use to access the command menu. You can access the menu from the serial console, or from an SSH client to the management interface.

To access the command menu from the serial console

1. From the serial console connected to the CONSOLE port, type the following key sequence.

   ```
   Esc (
   ```

2. The command menu opens.
   For details about each option on the command menu, see *Using the command menu*, on page 3-5.

To access the command menu using SSH

Before you can access the command menu using SSH, you must also have an IP address configured for remote lights-out management. For more information, see *Setting up remote lights-out SSH access*, on page 3-4.

1. Open the SSH client on a management workstation connected to the MGMT port on the BIG-IP system.
2. Type the following command, where **<IP addr>** is the IP address you configured for the lights-out system.

   ```
   ssh console@<ip addr>
   ```

3. The host console shell opens.
4. To open the command menu, type the following key sequence.

   ```
   Esc (
   ```

   For details about each option on the command menu, see *Using the command menu*, on page 3-5.

Setting up remote lights-out SSH access

You can use the command menu to set up remote SSH access to the BIG-IP system. To set up remote access, run the SCCP network configuration utility to configure an IP address, netmask, and gateway for the lights-out system. You can only connect remotely with the SSH client through the management network connected to the management port (MGMT).

To configure remote SSH lights-out access

1. Log into the BIG-IP system through the serial console.
2. Type the following key sequence.

   ```
   Esc (
   ```

3. After the command menu opens, type **N**.
   This starts the network configuration utility for the SCCP.
4. Add an IP address, netmask, and gateway on the management network.

Using out-of-band management commands

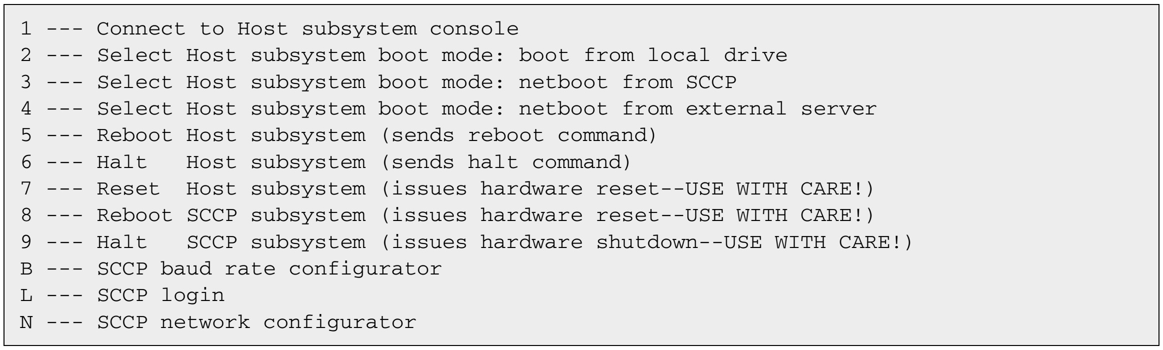
The host console shell implements a subset of the Microsoft standard out-of-band management protocol. These commands provide the ability to use a series of key strokes to manage the host processor. Table 3.1 lists the key-stroke options that are available.

Keystroke combination	Result
Esc + R + Esc + r + Esc + R	You can use this sequence during pass-through mode to reboot the platform. We do not recommend using this method to reboot the platform.
Esc (	Brings up the command menu.

Table 3.1 *Out-of-band management key combinations*

Using the command menu

The command menu provides the lights-out management options for the system (Figure 3.1).



```
1 --- Connect to Host subsystem console
2 --- Select Host subsystem boot mode: boot from local drive
3 --- Select Host subsystem boot mode: netboot from SCCP
4 --- Select Host subsystem boot mode: netboot from external server
5 --- Reboot Host subsystem (sends reboot command)
6 --- Halt   Host subsystem (sends halt command)
7 --- Reset  Host subsystem (issues hardware reset--USE WITH CARE!)
8 --- Reboot SCCP subsystem (issues hardware reset--USE WITH CARE!)
9 --- Halt   SCCP subsystem (issues hardware shutdown--USE WITH CARE!)
B --- SCCP baud rate configurator
L --- SCCP login
N --- SCCP network configurator
```

Figure 3.2 *A console view of the host processor console command menu*

Each of these options is described in Table 3.2. Note that some of these commands are not intended for use by end users. Table 3.2 also specifies which commands are not recommended for use by users.

Option	Description
1	Exits the command menu and returns to terminal emulation mode.
2	Configures the BIG-IP traffic management system to boot from the local hard drive or CompactFlash card.
3	Configures the host subsystem to netboot from the host subsystem processor. This option is only for factory testing.
4	Configures the SCCP to netboot the host processor from an external server attached to the management network interface. This option provides the ability to start the PXE installation process remotely.
5	Reboots the host subsystem. In this case, the BIG-IP traffic management operating system (TMOS) is rebooted.
6	Halts the host subsystem. In this case, the BIG-IP traffic management operating system (TMOS) is halted.
7	Resets the host subsystem. In this case, the system is reset with a hardware reset.
8	Reboots the switch card control processor (SCCP). This resets the entire unit.
9	Halts the switch card control processor (SCCP). This shuts down the entire unit.

Table 3.2 *Command menu options*

Option	Description
B	Runs the switch card control processor (SCCP) baud rate configuration utility. This utility provides the ability to configure the SCCP serial speed and parameters. This option is only available through the front panel serial console.
L	Presents a login prompt for the switch card control processor (SCCP) subsystem. This subsystem cannot be configured by end users. This option is only available through the front panel serial console.
N	Runs the switch card control processor (SCCP) network configuration utility. This utility provides the ability to reconfigure the IP address, netmask, and default gateway used by the SCCP. If you change these settings, your session is disconnected. This option is only available through the front panel serial console.

Table 3.2 *Command menu options*

◆ **Important**

We do not recommend using the reset option, option ***7****, under normal circumstances. It does not allow for graceful shutdown of the BIG-IP system.*

4

Configuring the BIG-IP Platform and General Properties

- Introducing the BIG-IP platform and general properties
- Configuring platform properties
- Configuring general properties

Introducing the BIG-IP platform and general properties

Part of managing a BIG-IP system involves configuring and maintaining a certain set of system properties. These properties fall into two main categories:

- General platform properties such as the BIG-IP system host name, IP address, and passwords for its system administrative accounts
- Device and local-traffic properties, such as NTP, DNS, and persistence settings

When you configure platform and device-related properties, you are affecting the operation of the BIG-IP system as a whole, rather than just one aspect of it. Similarly, when you configure the properties related to local traffic, you are globally affecting the operation of the local traffic management system.

◆ **Note**

For detailed information on configuring specific features of local traffic management, see the ***Configuration Guide for Local Traffic Management****.*

The remainder of this chapter describes how to configure and maintain these platform and general properties so that you can tailor the BIG-IP system to fit your needs exactly.

Configuring platform properties

When you configure platform properties, you configure settings such as the the IP address of the management port, the host name of the BIG-IP system, the host IP address, and user account passwords.

You can also view information about the device certificate, as well as import or export the certificate.

Configuring platform properties and user administration settings

From the General screen, you can configure general platform properties and user administration settings. Note that you can also configure many of these properties and settings by running the Setup utility.

Configuring general platform properties

You can configure these general properties for the BIG-IP system platform:

- An IP address, netmask, and route for the management interface
- The host name for the BIG-IP system
- The host IP address for the BIG-IP system
- Whether the BIG-IP system is a single device or part of a redundant system
- The unit ID, if the system is part of a redundant system
- The time zone in which the BIG-IP system operates

The following procedure provides the basic steps for configuring platform-related general properties. Following the procedure is a description of each property, along with additional details you might need for completing step 4 of the procedure.

To configure general platform properties

1. On the Main tab of the navigation pane, expand **System**, and click **Platform**.
   The General screen opens.

2. For the **Management Port** setting, type an IP address, a netmask, and a route address.

3. In the **Host Name** box, type a unique name for the BIG-IP system.

4. Configure all other general property settings as needed.
   For more information, see the sections following this procedure, as well as the online help.

5. At the bottom of the screen, click **Update**.

Configuring the management interface

Every BIG-IP system has a management port, or interface, named **MGMT.** The ***management interface*** is a special interface that the BIG-IP system uses to receive or send certain types of administrative traffic. You cannot use the management interface for normal traffic that is slated for load balancing. Instead, the BIG-IP system always uses the TMM switch interfaces for that type of traffic. ***TMM switch interfaces*** are those interfaces controlled by the Traffic Management Microkernel (TMM) service.

Configuring the management interface of a BIG-IP system means assigning an IP address to the interface, supplying a netmask for the IP address, and specifying an IP address for the BIG-IP system to use as a default route. The IP address that you assign to the management interface must be on a different network than the self IP addresses that you assign to VLANs. Note that specifying a default route for the management interface is only necessary if you intend to manage the BIG-IP system from a node on a different subnetwork.

To configure the management interface, you use the **Management Port** setting on the General screen. There are no default values for this setting.

◆ **Note**

The IP address for the management port must be in IPv4 format.

◆ **Tip**

You can also configure the management port using the LCD menu on the IP switch hardware. If you configure the management port using the LCD menu, you do not need to configure the port with the Configuration utility.

For procedural information on configuring the management interface, see the guide ***Installation, Licensing, and Upgrades for BIG-IP® Systems***. For information on the way that the TMM service affects the management interface, see the description of the TMM service in Chapter 18, *Configuring BIG-IP System Services*.

Supplying a host name

Every BIG-IP system must have a host name. Using the **Host Name** setting, type a fully qualified domain name for the BIG-IP system. An example of a host name is **mybigip.win.net**.

Assigning a host IP address

Every BIG-IP system must have a host IP address. This IP address can be the same as the address that you used for the management port, or you can assign a unique address.

To assign the host IP address, locate the **Host IP address** setting and select either **Use Management Port IP Address** or **Custom Host IP address**. The default value is **Use Management Port IP Address**.

Configuring high availability

You can use the general properties screen to specify whether the BIG-IP system is to operate as a single device or as part of a redundant system. The default value is **Single Device**.

To designate the BIG-IP system as being part of a redundant system, use the **High Availability** setting to select **Redundant Pair**. Then use the **Unit ID** setting to select the unit ID that you want to assign to the BIG-IP system (**1** or **2**).

Specifying a time zone

Another of the general platform properties that you can specify is the time zone. The many time zones that you can choose from are grouped into these categories: Africa, America, Antarctica, Arctic, Asia, Atlantic, Australia, Europe, Indian, and Pacific.

To set the time zone, use the **Time Zone** setting to select a time zone from the list. Select the time zone that most closely represents the location of the BIG-IP system you are configuring.

Specifying user administration settings

Part of managing platform-related properties is maintaining passwords for the system accounts, as well as enabling the **support** account. You can also configure the system to allow certain IP addresses to access the BIG-IP system through SSH.

Changing administrative account passwords

When you ran the Setup utility on the BIG-IP system, you set up some administrative accounts. Specifically, you set up the **root**, **admin**, and **support** accounts. The **root** and **admin** accounts are for use by BIG-IP system administrators, while the **support** account is for F5 Networks support personnel who require access to the customer’s system for troubleshooting purposes.

Users logging in with the **root** account have console-only access to the BIG-IP system. Users logging in with the **admin** account have browser-only access to the BIG-IP system.

You can use the General screen of the platform properties to change the passwords for **root** and **admin** accounts on a regular basis. To change a password, locate the **Root Account** or **Admin Account** setting, and in the **Password** box, type a new password. In the **Confirm** box, retype the same password. For more information, see *To configure general platform properties*, on page 4-2.

Enabling the Support account

The **support** account is an optional account that you can enable on the BIG-IP system. When you enable this account, authorized F5 Networks support personnel can access the BIG-IP system to perform troubleshooting.

To enable the **support** account, find the **Support Account** setting and select **Enabled**. Then type a password, once in the **Password** box and again in the **Confirm** box.

Configuring SSH access

When you configure SSH access, you enable user access to the BIG-IP system through SSH. Also, only the IP addresses that you specify are allowed access to the system using SSH.

To configure SSH access, locate the **SSH Access** setting and click the **Enabled** box. Then use the **SSH IP Allow** setting to select either * **All Addresses** or **Specify Range**, which allows you to specify a range of addresses.

Managing a device certificate

Sometimes, multiple BIG-IP systems need to communicate securely over a network. For example, multiple BIG-IP systems might need to collect performance data over a wide area network, for global traffic management. In this case, these BIG-IP systems need to exchange SSL certificates and keys to ensure secure data communication. These certificates are separate from the SSL certificates that you install for managing (that is, terminating and initiating) local SSL traffic. For information on requesting and installing certificates to manage local SSL traffic, see the ***Configuration Guide for Local Traffic Management***.

You can view information about a device certificate that is currently installed on the BIG-IP system. You can also export a certificate or import a different certificate.

Viewing certificate and key information

You can use the Configuration utility to view information about any SSL certificate and key that you have installed on the BIG-IP system. The specific information you can view about a certificate is:

- Name
- Subject
- Expiration date
- Version
- Serial number (if any)
- Common Name
- Division
- Locality, state or province, and country
- Issuer

To view device certificate and key information

1. On the Main tab of the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of any self-signed certificate.
2. On the menu bar, click **Device Key**.
   This displays the type and size of the key.
3. On the menu bar, click **Trusted Device Certificates**.
   This displays the properties of any certificates signed by a trusted certificate authority (CA). If no trusted certificate exists, the value of the **Subject** property shows **No certificate**.

Importing, exporting, or renewing a device certificate

You can import, export, or renew two kinds of certificates: a device certificate or a trusted device certificate.

To import a device certificate

1. On the Main tab of the navigation pane, expand **System** and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. At the bottom of the screen, click **Import**.
   This displays the screen for importing either a certificate, or a certificate and key.
3. From the **Import Type** list, select an import type, either **Certificate** or **Certificate and Key**.
4. From the **Certificate Source** setting, click either **Upload File** or **Paste Text**:
   - If you click **Upload File**, type a file name or click **Browse**.
     If you click **Browse**:

     a) Navigate to the relevant Windows folder and click a file name.

     b) On the browser window, click **Open**.
   - If you click **Paste Text**:

     a) Copy the text from another source.

     b) Paste the text into the **Certificate Source** window.
5. Click **Import**.

To import a trusted device certificate

1. On the Main tab of the navigation pane, expand **System** and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. On the menu bar, click **Trusted Device Certificates**.
   This displays the properties of a trusted CA certificate.

3. At the bottom of the screen, click **Import**.
   This displays the properties of a trusted CA certificate.
4. From the **Import Method** list, select an import method.
5. From the **Certificate Source** setting, click either **Upload File** or **Paste Text**:
   - If you click **Upload File**, type a file name or click **Browse**.
     If you click **Browse**:

     a) Navigate to the relevant Windows folder and click a file name.

     b) On the browser window, click **Open**.
   - If you click **Paste Text**:

     a) Copy the text from another source.

     b) Paste the text into the **Certificate Source** window.
6. Click **Import**.

To export a device certificate

1. On the Main tab of the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. If you want to export a trusted CA certificate, click **Trusted Device Certificates** on the menu bar.
3. At the bottom of the screen, click **Export**.
   The screen displays the text of the existing certificate.
4. Next to the **Certificate File** setting, click **Download <certificate_name>**.

To renew a device certificate

1. On the Main tab of the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. If you want to renew a trusted CA certificate, click **Trusted Device Certificates** on the menu bar.
3. At the bottom of the screen, click **Renew**.
   This displays the properties of the certificate and its associated key.
4. Change any properties as needed.
   For detailed information, see the online help.
5. Click **Finished**.

Importing and exporting a key

You can use the Configuration utility to import and export keys.

To import a key

1. On the Main tab of the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. On the menu bar, click **Device Key**
   This displays the properties of the key.
3. Click **Import**.
4. From the **Import Type** list, select an import type, either **Certificate** or **Certificate and Key**.
5. From the **Key Source** setting, click either **Upload File** or **Paste Text**:
   - If you click **Upload File**, type a file name or click **Browse**.
     If you click **Browse**:

     a) Navigate to the relevant Windows folder and click a file name.

     b) On the browser window, click **Open**.
   - If you click **Paste Text**:

     a) Copy the text from another source.

     b) Paste the text into the **Key Source** window.
6. Click **Import**.

To export a key

1. On the Main tab of the navigation pane, expand **System**, and click **Device Certificates**.
   This displays the properties of a self-signed certificate.
2. On the menu bar, click **Device Key**.
   This displays the properties of the key.
3. Click **Export**.
   The screen displays the text of the key.
4. Next to the **Key File** setting, click **Download <key_name>**.

Configuring general properties

Using the Configuration utility, you can view and configure a number of general BIG-IP system properties. Some of these properties are related to the BIG-IP system as a device, while others are related to local traffic management.

Configuring device-related properties

You can view or configure a number of properties related to the BIG-IP system as a device. These properties fall into three main categories: general device properties, Network Time Protocol (NTP) properties, and Domain Name System (DNS) properties.

Configuring general properties

The BIG-IP general properties that you can view are:

- The host name
- The BIG-IP software version number
- The number of CPUs available
- The number of CPUs that are active
- The current CPU mode (uniprocessor or multiprocessor)

The BIG-IP general properties that you can configure are:

- Network boot
- Quiet boot
- The percent of memory usage for reboot

The following procedure provides the basic steps for configuring general properties. Following the procedure are descriptions of the properties that you might need for completing step 2 of the procedure.

To view or configure general properties

1. On the Main tab of the navigation pane, expand **System**, and click **General Properties**.
   The General screen opens.
2. View or configure any settings.
   For detailed information on these settings, see the online help and Table 4.1, on page 4-10.
3. If you configured any settings, click **Update**.

Table 4.1, on page 4-10 lists and describes the general properties that you can view or configure.

Property	Description	Default Value
Host Name	Displays the host name of the BIG-IP system. This name is the same host name that you specified on the main Platform screen.	No default value
Version	Displays the version number of the BIG-IP system software that is running on the system.	No default value
CPU Count	Displays the total number of CPUs that the BIG-IP system contains.	No default value
Active CPUs	Displays the total number of CPUs that are currently active on the BIG-IP system.	No default value
CPU Mode	Displays the current processor mode of the system, either uniprocessor or multiprocessor.	No default value
Network Boot	Enables or disables the network boot feature. If you enable this feature and then reboot the system, the system boots from an ISO image on the network, rather than from an internal media drive. Use this option only when you want to install software on the system, for example, for an upgrade or a re-installation. Note that this setting reverts to **Disabled** after you reboot the system a second time.	Disabled (unchecked)
Quiet Boot	Enables or disables the quiet boot feature. If you enable this feature, the system suppresses informational text on the console during the boot cycle.	Enabled (checked)
Memory Restart Percent	Specifies the memory usage percent at which the system reboots.	97

Table 4.1 *General properties of a BIG-IP system device*

Configuring NTP

Network Time Protocol (NTP) is a protocol that synchronizes the clocks on a network. You can use the Configuration utility to specify a list of IP addresses of the servers that you want the BIG-IP system to use when updating the time on network systems. You can also edit or delete the entries in the server list.

To configure a list of NTP time servers

1. On the Main tab of the navigation pane, expand **System**, and click **General Properties**.
   The General screen opens.

2. From the Device menu, choose NTP.
   This opens the NTP screen.

3. For the **Time Server List** setting, add, edit, or remove an IP address:

- To add an IP address to the list:

  a) Type a time server's IP address or host name in the **Address** box.

  b) Click **Add**.

- To edit an IP address in the list:

  a) In the **Time Server List** area, select an IP address.
  The IP address appears in the **Address** box.

  b) In the **Address** box, change the IP address.

  c) Click the **Edit** button.

- To remove an IP address from the list:

  a) In the **Time Server List** area, select an IP address.
  The IP address appears in the **Address** box.

  b) Click the **Delete** button.

4. Click **Update**.

Configuring DNS

Domain Name System (DNS) is an industry-standard distributed internet directory service that resolves domain names to IP addresses. If you plan to use DNS in your network, you can use the Configuration utility to configure DNS for the BIG-IP system.

When you configure DNS, you create two lists: a DNS lookup server list, and a BIND forwarder server list. The ***DNS lookup server list*** allows BIG-IP system users to use IP addresses, host names, or fully-qualified domain names (FQDNs) to access virtual servers, nodes, or other network objects.

The ***BIND forwarder server list*** provides DNS resolution for servers and other equipment load balanced by the BIG-IP system, that is, for the servers that the BIG-IP system uses for DNS proxy services.

◆ **Note**

*To use DNS Proxy services, you must enable the **named** service.*

In addition to adding servers to the DNS lookup server list and the BIND forwarder server list, you can also edit or delete the entries in these lists.

To configure DNS for the BIG-IP system

1. On the Main tab of the navigation pane, expand **System**, and click **General Properties**.
   The General screen opens.

2. From the Device menu, choose DNS.
   This opens the DNS screen.

3. In the **DNS Lookup Server List** area, you can add, edit, or remove a server IP address:
   - To add a server to the list:

     a) Type the IP address of a properly-configured name server in the **Address** box.

     b) Click **Add**.

     c) To add backup DNS servers to the list, repeat steps a and b.
   - To edit an IP address in the list:

     a) In the **DNS Lookup Server List** area, select an IP address. The IP address appears in the **Address** box.

     b) In the **Address** box, change the IP address.

     c) Click **Edit**.
   - To remove an IP address from the list:

     a) In the **DNS Lookup Server List** area, select an IP address. The IP address appears in the **Address** box

     b) Click **Delete**.
4. In the **BIND Forwarder Server List** area, you can add, edit, or remove a server IP address:
   - To add a server to the list:

     a) Type a server’s IP address in the **Address** box.

     b) Click **Add**.
   - To edit an IP address in the list:

     a) In the **BIND Forwarder Server List** area, select an IP address. The IP address appears in the **Address** box.

     b) In the **Address** box, change the IP address.

     c) Click **Edit**.
   - To remove an IP address from the list:

     a) In the **BIND Forwarder Server List** area, select an IP address. The IP address appears in the **Address** box

     b) Click **Delete**.
5. Click **Update**.

Configuring local-traffic properties

The BIG-IP system includes a set of properties that apply globally to the local traffic management system. These properties fall into two main categories: general local-traffic properties, and persistence properties. You can use the Configuration utility to configure and maintain these properties.

Configuring general local-traffic properties

You can configure a number of properties that affect the general behavior of the BIG-IP local traffic management system. In most cases, these properties are not directly related to any one type of local traffic management object, such as a virtual server or a load balancing pool.

The following procedure provides the basic steps for configuring general local-traffic properties. Following the procedure are descriptions of the properties with additional details you might need for completing step 3 of the procedure.

To configure general local-traffic properties

1. On the Main tab of the navigation pane, expand **System**, and click **General Properties**.
   The General screen opens.
2. From the Local Traffic menu, choose General.
3. Configure all properties or retain the default values.
   For detailed information, see Table 4.2.
4. Click **Update**.

Table 4.2 lists and describes the properties that you can configure to manage the behavior of the local traffic management system.

Property	Description	Default Value
Auto Last Hop	Specifies, when checked (enabled), that the system automatically maps the last hop for pools.	Enabled (checked)
Maintenance Mode	Specifies, when checked (enabled), that the unit is in maintenance mode. In maintenance mode, the system stops accepting new connections and slowly completes the processing of existing connections.	Disabled (unchecked)
VLAN-Keyed Connections	Check this setting to enable VLAN-keyed connections. VLAN-keyed connections are used when traffic for the same connection must pass through the system several times, on multiple pairs of VLANs (or in different VLAN groups).	Enabled (checked)

Table 4.2 *General properties for globally managing local traffic*

Property	Description	Default Value
Path MTU Discovery	Specifies, when checked (enabled), that the system discovers the maximum transmission unit (MTU) that it can send over a path without fragmenting TCP packets.	Enabled (checked)
Reject Unmatched Packets	Specifies, when checked (enabled), that the system returns a TCP RESET or ICMP_UNREACH packet if no virtual servers on the system match the destination address of the incoming packet. When this setting is disabled, the system silently drops the unmatched packet.	Enabled (checked)
Maximum Node Idle Time	Specifies the number of seconds a node can be left idle by the Fastest load balancing mode. The system sends fewer connections to a node that is responding slowly, and periodically recalculates the response time of the slow node.	**0** (disabled)
Reaper High-water Mark	Specifies, in percent, the memory usage at which the system stops establishing new connections. Once the system meets the reaper high-water mark, the system does not establish new connections until the memory usage drops below the reaper low-water mark. To disable the adaptive reaper, set the high-water mark to **100**. ***Note:*** *This setting helps to mitigate the effects of a denial-of-service attack.*	**95**
Reaper Low-water Mark	Specifies, in percent, the memory usage at which the system silently purges stale connections, without sending reset packets (RST) to the client. If the memory usage remains above the low-water mark after the purge, then the system starts purging established connections closest to their service timeout. To disable the adaptive reaper, set the low-water mark to **100**.	**85**
SYN Check^{TM} Activation Threshold	Specifies the number of new or untrusted TCP connections that can be established before the system activates the SYN Cookies authentication method for subsequent TCP connections.	**16384**
Layer 2 Cache Aging Time	Specifies, in seconds, the amount of time that records remain in the Layer 2 forwarding table, when the MAC address of the record is no longer detected on the network.	**300**

Table 4.2 *General properties for globally managing local traffic*

Property	Description	Default Value
Share Single MAC Address	Specifies, when checked (enabled), that all VLANs share a single MAC address. If you use the default value (unchecked), the BIG-IP gives each VLAN the MAC address of the VLAN's lowest-numbered interface. Use this setting when configuring an active/standby redundant system.	Disabled (unchecked)
SNAT Packet Forwarding	Specifies the type of traffic for which the system attempts to forward (instead of reject) Any-IP packets, when the traffic originates from a member of a SNAT. There are two possible values: **TCP and UDP Only**: Specifies that the system forwards, for TCP and UDP traffic only, Any-IP packets originating from a SNAT member. **All Traffic**: Specifies that the system forwards, for all traffic types, Any-IP packets originating from a SNAT member.	**TCP and UDP Only**

Table 4.2 *General properties for globally managing local traffic*

Configuring persistence properties

Using the Configuration utility, you can perform certain persistence-related tasks such as managing the way that destination IP addresses are stored in the persistence table, and specifying a data group that contains proxy IP addresses.

The following procedure provides the basic steps for configuring general persistence-related properties. Following the procedure are descriptions of the properties with additional details you might need for completing step 3 of the procedure.

To configure persistence properties

1. On the Main tab of the navigation pane, expand **System**, and click **General Properties**.
   The General screen opens.
2. From the Local Traffic menu, choose Persistence.
3. Configure the properties or retain the default values.
   For detailed information, see Table 4.3, on page 4-16.
4. Click **Update**.

Table 4.3 lists and describes the properties that you can configure to manage general persistence-related properties.

Property	Description	Default Value
Management of Destination Address Entries	Specifies how the system manages the destination IP address entries in the persistence table. **Timeout**: Specifies that entries remain in the persistence table until the BIG-IP system times them out, based on the timeout value configured in the corresponding persistence profile. **Maximum Entries**: Specifies that the system stops adding entries to the persistence table when the number of entries reaches the maximum number of entries allowed.	**Timeout**
Proxy Address Data Group	Specifies the data group that contains proxy IP addresses. You use this data group to identify the addresses that are to be treated as proxies when you enable the **Map Proxies** option on a persistence profile.	**aol**

Table 4.3 *General properties for controlling session persistence*

5

Configuring VLANs and VLAN Groups

- Introducing virtual LANs
- Creating and managing VLANs
- Creating and managing VLAN groups
- Assigning self IPs to VLANs and VLAN groups

Introducing virtual LANs

In Chapter 1, *Introducing BIG-IP Network and System Management*, we described the BIG-IP system as being a multilayer switch instead of a standard IP router. This allows you to create and deploy virtual local area networks (VLANs). A ***VLAN*** is a logical subset of hosts on a local area network (LAN) that operate in the same IP address space. Grouping hosts together in a VLAN has distinct advantages. For example, with VLANs, you can:

- Reduce the size of broadcast domains, thereby enhancing overall network performance.
- Reduce system and network maintenance tasks substantially. Functionally-related hosts no longer need to physically reside together to achieve optimal network performance.
- Enhance security on your network by segmenting hosts that must transmit sensitive data.

The way that you group hosts into VLANs is by using the Configuration utility to create a VLAN and associate physical interfaces with that VLAN. In this way, any host that sends traffic to a BIG-IP system interface is logically a member of the VLAN or VLANs to which that interface belongs.

Understanding VLANs on a BIG-IP system

The BIG-IP system is a port-based switch that includes multilayer processing capabilities. These capabilities enhance standard VLAN behavior, in these ways:

- You can associate physical interfaces on the BIG-IP system directly with VLANs. In this way, you can associate multiple interfaces with a single VLAN, or you can associate a single interface with multiple VLANs.
- You do not need physical routers to establish communication between separate VLANs. Instead, the BIG-IP system can process messages between VLANs.
- You can incorporate a BIG-IP system into existing, multi-vendor switched environments, due to the BIG-IP system's compliance with the IEEE 802.1q VLAN standard.
- You can combine two or more VLANs into an object known as a VLAN group. With a ***VLAN group***, a host in one VLAN can communicate with a host in another VLAN using a combination of layer 2 forwarding and IP routing. This offers both performance and reliability benefits.

Understanding the default VLAN configuration

By default, the BIG-IP system includes two VLANs, named **internal** and **external**. When you initially ran the Setup utility, you assigned the following to each of these VLANs:

- A static and a floating self IP address
- A VLAN tag
- One or more BIG-IP system interfaces

A typical VLAN configuration is one in which you create the two VLANs **external** and **internal**, and one or more BIG-IP system interfaces assigned to each VLAN. You then create a virtual server, and associate a default load balancing pool with that virtual server. Figure 5.1 shows a typical configuration using the default VLANs **external** and **internal**.

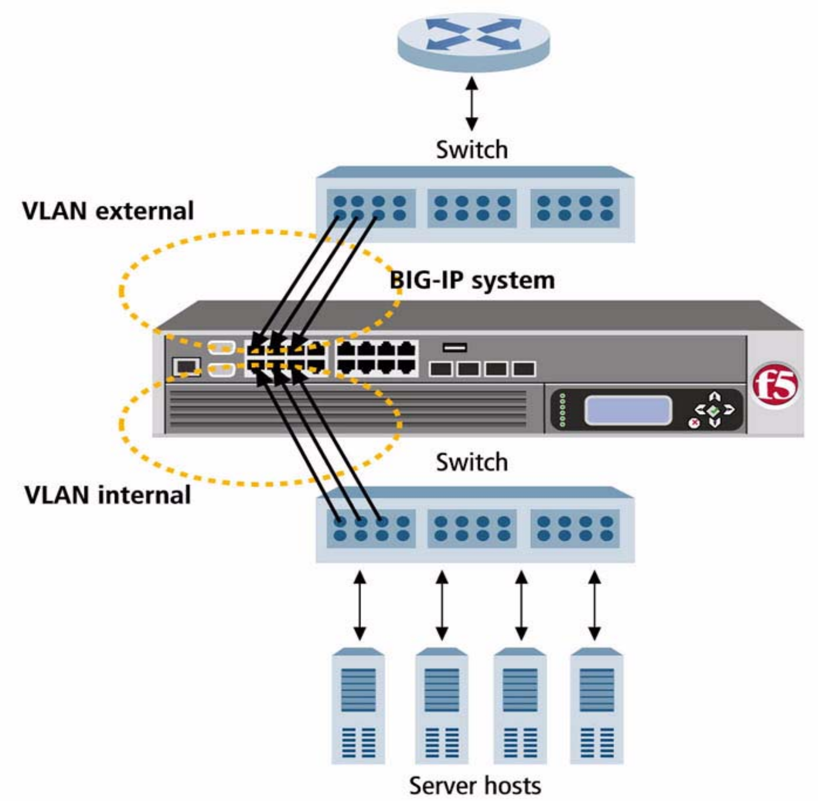


Figure 5.1 *A typical configuration using the default VLANs*

Every VLAN must have a static self IP address associated with it. The ***self IP address*** of a VLAN represents an address space, that is, the range of IP addresses pertaining to the hosts in that VLAN. When you ran the Setup utility earlier, you assigned one static self IP address to the VLAN **external**, and one static self IP address to the VLAN **internal**. When sending a request to a destination server, the BIG-IP system can use these self IP addresses to determine the specific VLAN that contains the destination server.

For example, suppose the self IP address of VLAN **external** is **12.1.0.100,** and the self IP address of the VLAN **internal** is **11.1.0.100,** and both self IP addresses have a netmask of **255.255.0.0**. If the IP address of the destination server is **11.1.0.20**, then the BIG-IP system can compare the self IP addresses to the host's IP address to determine that the destination server is in the VLAN **internal**. This process, combined with checking the ARP cache and a VLAN's L2 forwarding table, ensures that the BIG-IP system successfully sends the request to the destination server.

◆ **Note**

*By default, the MAC address that the BIG-IP system assigns to a VLAN self IP address is the MAC address of the lowest-numbered interface associated with that VLAN. You can change this behavior by configuring the bigdb™ configuration key **Vlan.MacAssignment**. For more information, see the man page for the **bigpipe db** command.*

Creating and managing VLANs

When you create a VLAN, you assign a name and an identifying tag to the VLAN. Then you associate one or more BIG-IP system interfaces with the VLAN. Also, if the BIG-IP system is a unit of a redundant system, you can specify a special MAC address that the two units share, as a way to ensure that connections are successfully processed when failover occurs. Finally, you can specify that you want the BIG-IP system to use VLAN-related events to trigger failover in a redundant-system configuration.

To create a VLAN, you use the Configuration utility. For information on managing an existing VLAN, see *Managing a VLAN*, on page 5-10.

Creating a VLAN

The BIG-IP system offers several settings that you can configure for a VLAN. These settings are summarized in Table 5.1.

Setting	Description	Default Value
Name	Specifies a unique name for the VLAN. This value is required.	No default value
Tag	Specifies the VLAN ID. If you do not specify a VLAN ID, the BIG-IP system assigns an ID automatically. The value of a VLAN tag can be between **1** and **4094**.	No default value

Table 5.1 *Configuration settings for a VLAN*

Setting	Description	Default Value
Interfaces	Specifies any tagged or untagged interfaces or trunks that you want to associate with the VLAN.	No default value
Source Check	Causes the BIG-IP system to verify that the return path of an initial packet is through the same VLAN from which the packet originated.	Unchecked
MTU	Specifies the maximum transmission unit for the VLAN.	**1500**
MAC Masquerade	Sets up a media access control (MAC) address that is shared by a redundant system.	No default value
Fail-safe	Triggers fail-over in a redundant system when certain VLAN-related events occur.	Unchecked

Table 5.1 *Configuration settings for a VLAN*

Use the following procedure to create a VLAN. For detailed information about each setting, see the sections following the procedure.

◆ **Important**

*In addition to configuring the settings listed in Table 5.1, you must also assign a self IP address to the VLAN. For more information, see **Assigning self IPs to VLANs and VLAN groups**, on page 5-18, and Chapter 6, **Configuring Self IP Addresses**.*

To create a VLAN

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.

2. In the upper-right corner, click **Create**.
   The VLANs screen opens.

3. Locate the General Properties area, and in the **Name** box, type a unique name for the VLAN.

4. In the **Tag** box, type a tag for the VLAN, or leave the box blank. If you do not specify a tag, the BIG-IP system assigns one automatically.

5. In the Resources area, for the **Interfaces** setting, click an interface number or trunk name in the **Available** box, and using a Move button (**<<** or **>>**), move the interface number to the **Untagged** or **Tagged** box. Repeat this step as necessary.
   For more information on tagged and untagged interfaces, see *Assigning interfaces to a VLAN*, on page 5-5.

6. If you want to enable source checking, then in the Configuration area, click the **Source Check** box.

7. For the **MTU** setting, use the default value or type a new value.

8. In the **MAC Masquerade** box, type a MAC address.
   For more information, see *Specifying a MAC masquerade address*, on page 5-8.

9. For the **Fail-safe** setting, check the box if you want to base redundant-system failover on VLAN-related events.
   For more information, see Chapter 13, *Setting up a Redundant System*.

10. Click **Finished**.

Specifying a VLAN name

When creating a VLAN, you must assign it a unique name. Once you have finished creating the VLAN, the VLAN name appears in the list of existing VLANs.

Specifying a VLAN tag

A VLAN ***tag*** is a unique ID number that you assign to a VLAN. If you do not explicitly assign a tag to a VLAN, the BIG-IP system assigns a tag automatically. The value of a VLAN tag can be between **1** and **4094**. Once you or the BIG-IP assigns a tag to a VLAN, any message sent from a host in that VLAN includes this VLAN tag as a header in the message.

A VLAN tag is useful when an interface has multiple VLANs associated with it; that is, when the interfaces you assigned to the VLAN are assigned as tagged interfaces. In this case, the BIG-IP system can read the VLAN tag in the header of a message to determine the specific VLAN in which the source or destination host resides. For more information on tagged interfaces, see *Tag-based access to VLANs*, on page 5-6.

◆ **Important**

If the device connected to a BIG-IP system interface is another switch, the VLAN tag that you assign to the VLAN on the BIG-IP system interface must match the VLAN tag assigned to the VLAN on the interface of the other switch.

Assigning interfaces to a VLAN

For each VLAN that you create, you must assign one or more BIG-IP system interfaces to that VLAN, using the **Interfaces** setting. When you assign an interface to a VLAN, you indirectly control the hosts from which the BIG-IP system interface sends or receives messages.

◆ **Tip**

*You can use the **Interfaces** setting to assign not only individual interfaces to the VLAN, but also trunks. Any trunks that you create are automatically included for selection in the list of available interfaces. For more information on trunks, see Chapter 10, **Working with Trunks**.*

For example, if you assign interface 1.11 to VLAN **A**, and you then associate VLAN A with a virtual server, then the virtual server sends its outgoing traffic through interface 1.11, to a destination host in VLAN **A**. Similarly, when a destination host sends a message to the BIG-IP system, the host's VLAN membership determines the BIG-IP system interface that should receive the incoming traffic.

Each VLAN has a MAC address. The MAC address of a VLAN is the same MAC address of the lowest-numbered interface assigned to that VLAN.

The BIG-IP system supports two methods for sending and receiving messages through an interface that is a member of one or more VLANs. These two methods are port-based access to VLANs and tag-based access to VLANs. The method used by a VLAN is determined by the way that you add a member interface to a VLAN.

Port-based access to VLANs

With port-based access to VLANs, the BIG-IP system accepts frames for a VLAN simply because they are received on an interface that is a member of that VLAN. With this method, an interface is an untagged member of the VLAN. Frames sent out through ***untagged*** interfaces contain no tag in their header.

Port-based access to VLANs occurs when you add an interface to a VLAN as an untagged interface. In this case, the VLAN is the only VLAN that you can associate with that interface. This limits the interface to accepting traffic only from that VLAN, instead of from multiple VLANs. If you want to give an interface the ability to accept and receive traffic for multiple VLANs, you add the same interface to each VLAN as a tagged interface. The following section describes tagged interfaces.

Tag-based access to VLANs

With tag-based access to VLANs, the BIG-IP system accepts frames for a VLAN because the frames have tags in their headers and the tag matches the VLAN identification number for the VLAN. An interface that accepts frames containing VLAN tags is a ***tagged member*** of the VLAN. Frames sent out through tagged interfaces contain a tag in their header.

Tag-based access to VLANs occurs when you add an interface to a VLAN as a tagged interface. You can add the same tagged interface to multiple VLANs, thereby allowing the interface to accept traffic from each VLAN with which the interface is associated.

When you add an interface to a VLAN as a tagged interface, the BIG-IP system associates the interface with the VLAN identification number, or ***tag***, which becomes embedded in a header of a frame.

◆ **Note**

*Every VLAN has a tag. You can assign the tag explicitly when creating the VLAN, or the BIG-IP system assigns it automatically if you do not supply one. For more information on VLAN tags, see **Specifying a VLAN tag**, on page 5-5.*

Each time you add an interface to a VLAN, either when creating a VLAN or modifying its properties, you can designate that interface as a tagged interface. A single interface can therefore have multiple tags associated with it.

The result is that whenever a frame comes into that interface, the interface reads the tag that is embedded in a header of the frame. If the tag in the frame matches any of the tags associated with the interface, the interface accepts the frame. If the tag in the frame does *not* match any of the tags associated with the interface, the interface rejects the frame.

Example

Figure 5.2 shows the difference between using three untagged interfaces (where each interface must belong to a separate VLAN) versus one tagged interface (which belongs to multiple VLANs).

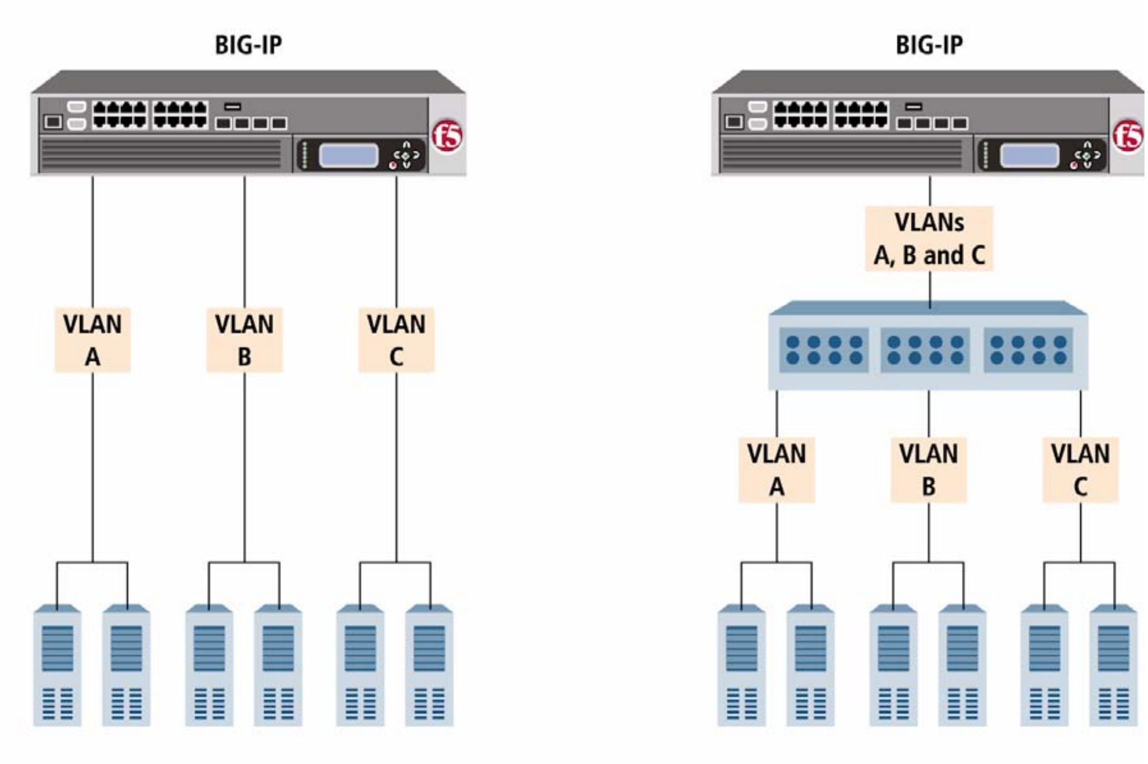


***Figure 5.2** Equivalent solutions using untagged and tagged interfaces*

The configuration on the left shows a BIG-IP unit with three internal interfaces, each a separate, untagged interface. This is a typical solution for supporting three separate customer sites. In this scenario, each interface can accept traffic only from its own VLAN.

Conversely, the configuration on the right shows a BIG-IP system with one internal interface and an external switch. The switch places the internal interface on three separate VLANs. The interface is configured on each VLAN as a tagged interface. In this way, the single interface becomes a tagged member of all three VLANs, and accepts traffic from all three. The configuration on the right is the functional equivalent of the configuration on the left.

◆ **Important**

If you are connecting another switch into a BIG-IP system interface, the VLAN tag that you assign to the VLAN on the BIG-IP system must match the VLAN tag on the interface of the other switch.

Enabling source checking

When you enable the **Source Check** setting, the BIG-IP system verifies that the return path for an initial packet is through the same VLAN from which the packet originated. The system performs this verification only if you check the **Source Check** box for the VLAN, and if the global setting **Auto Last Hop** is not enabled. For information on the **Auto Last Hop** setting, see Chapter 4, *Configuring the BIG-IP Platform and General Properties*.

Specifying the maximum transmission units

The value of the maximum transmission unit, or ***MTU***, is the largest size that the BIG-IP system allows for an IP datagram passing through a BIG-IP system interface. The default value is **1500**.

Specifying a MAC masquerade address

Every VLAN has a media access control (MAC) address that corresponds to the VLAN’s self IP address. The MAC address of a VLAN is the MAC address of the lowest-numbered interface assigned to that VLAN. For example, if the lowest-numbered interface assigned to VLAN **internal** is 3.1, and the MAC address of that interface is **0:0:0:ac:4c:a2**, then the MAC address of VLAN **internal** is also **0:0:0:ac:4c:a2**.

A ***MAC masquerade address*** is a variation of the VLAN’s MAC address, and this address is shared between two units of a redundant system. When you specify a MAC masquerade address, a destination server sending a response to the BIG-IP system sends its response to the VLAN’s MAC masquerade address, instead of to the VLAN’s regular MAC address. The server accomplishes this by using the VLAN’s floating self IP address as the default route when sending responses to the BIG-IP system. (For more information on configuring a server to use a floating IP address as the default route, see Chapter 13, *Setting up a Redundant System*.)

Specifying a MAC masquerade address for a VLAN has the following advantages:

- Increased reliability and failover speed, especially in lossy networks
- Interoperability with switches that are slow to respond to the network changes
- Interoperability with switches that are configured to ignore network changes

When you assign a MAC masquerade address to a VLAN, the BIG-IP system automatically sends a gratuitous ARP message to the default router and other devices on the network. This gratuitous ARP message notifies these devices that the MAC address of the BIG-IP system interface assigned to the VLAN has changed to the MAC masquerade address.

The MAC masquerade address must be a unique address, in order to avoid frame collisions. The safest way to create a MAC masquerade address is to first determine the MAC address of the VLAN (that is, the MAC address of the lowest-numbered interface assigned to that VLAN), and then logically **OR** the first byte with **0x02**. This makes the MAC address a locally-administered MAC address.

Continuing with the example above where the VLAN's MAC address is **0:0:0:ac:4c:a2**, a MAC masquerade address of **02:0:0:ac:4c:a2** is suitable to use on both BIG-IP units in the redundant system. For help in finding the MAC address of a VLAN, see *To find the MAC address of a VLAN*, following.

◆ **Important**

We highly recommend that you set the MAC masquerade address to be the same on both the active and standby units.

To find the MAC address of a VLAN

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of existing VLANs.
2. Click a VLAN name.
   This displays the properties for that VLAN.
3. In the **Interfaces** setting, note the lowest-numbered interface assigned to the VLAN.
4. On the Main tab of the navigation pane, expand **Network** and click **Interfaces**.
   This displays a list of all BIG-IP system interfaces and their MAC addresses.
5. Locate the interface number that you noted on the VLAN's properties screen.
6. In the MAC Address column, view the MAC address for the interface.

After you have found the correct MAC address, create the MAC masquerade address using the procedure described in step 8 in *Creating a VLAN*, on page 5-3.

Specifying fail-safe

VLAN fail-safe is a feature you enable when you want to base redundant-system failover on VLAN-related events. For more information, see Chapter 13, *Setting up a Redundant System*.

Managing a VLAN

After you have created a VLAN, you can use the Configuration utility to modify its properties, delete the VLAN, or to maintain its layer 2 forwarding table.

Managing VLAN properties

Using the Configuration utility, you can modify all of the properties of a VLAN, except the VLAN name, the tag, and the MAC address with which the VLAN is associated (that is, the MAC address of the lowest-numbered interface that is assigned to the VLAN).

You can also use the Configuration utility to delete a VLAN.

To change VLAN properties

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.
2. Click the name of the VLAN you want to modify.
   This opens the properties screen for the VLAN.
3. Modify the values of any settings.
4. Click **Update**.

To delete a VLAN

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.
2. Check the Select box next to the VLAN name.
3. Click **Delete**.
   A confirmation query appears.
4. Click **Delete**.

Maintaining the L2 forwarding table

Layer 2 forwarding is the means by which frames are exchanged directly between hosts, with no IP routing required. This is accomplished using a simple forwarding table for each VLAN. The ***L2 forwarding table*** is a list that shows, for each host in the VLAN, the MAC address of the host, along with the interface that the BIG-IP system needs for sending frames to that host. The intent of the L2 forwarding table is to help the BIG-IP system determine the correct interface for sending frames, when the system determines that no routing is required.

The format of an entry in the L2 forwarding table is:

```
<MAC address> -> <if>
```

For example, an entry for a host in the VLAN might looks like this:

```
00:a0:c9:9e:1e:2f -> 2.1
```

The BIG-IP system learns the interfaces that correspond to various MAC entries as frames pass through the system, and automatically adds entries to the table accordingly. These entries are known as ***dynamic entries***. You can also add entries to the table manually, and these are known as ***static entries***. Entering static entries is useful if you have network devices that do not advertise their MAC addresses. The system does not automatically update static entries.

The BIG-IP system does not always need to use the L2 forwarding table to find an interface for frame transmission. For instance, if a VLAN has only one interface assigned to it, then the BIG-IP system automatically uses that interface.

Occasionally, the L2 forwarding table does not include an entry for the destination MAC address and its corresponding BIG-IP system interface. In this case, the BIG-IP system floods the frame through all interfaces associated with the VLAN, until a reply creates an entry in the L2 forwarding table.

Viewing the L2 forwarding table

You can use the Configuration utility to view the entries in the L2 forwarding table.

To view the L2 forwarding table

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.
2. Click the name of the VLAN you want to modify.
   This opens the properties screen for the VLAN.
3. On the menu bar, click **Layer 2 Static Forwarding Table**.
   This displays any entries currently in the L2 forwarding table.

Adding entries to the L2 forwarding table

You can add static entries to the L2 forwarding table when you want to give the BIG-IP system the ability to send messages to a specific host in the VLAN.

To add an entry to the L2 forwarding table

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.
2. Click the name of the VLAN you want to modify.
   This opens the properties screen for the VLAN.
3. On the menu bar, click **Layer 2 Static Forwarding Table**.
   This displays any entries currently in the L2 forwarding table.
4. Click **Create**.
   This displays the screen for adding entries to the table.
5. For the **Interfaces** setting, select an interface number.
6. In the **MAC Address** box, type the MAC address of the host to which the entry applies.
7. Click **Repeat** if you want to add another entry, or click **Finished**.

Setting the L2 forwarding aging time

Entries in the L2 forwarding table have a specified life span, after which they are removed if the MAC address is no longer present on the network. This life span is called the ***layer 2 cache aging time***. The default value is 300 seconds. Using the Configuration utility, you can change this value.

To change the layer 2 cache aging time

1. On the Main tab of the navigation pane, expand **System** and click **General Properties**.
   This displays a list of general properties for the BIG-IP system.
2. On the menu bar, from **Local Traffic**, choose General.
   This displays a list of general properties related to local traffic.
3. In the **Layer 2 Cache Aging Time** box, change the value.
4. Click **Update**.

Creating and managing VLAN groups

A ***VLAN group*** is a logical container that includes two or more distinct VLANs. VLAN groups are intended for load balancing traffic in a layer 2 network, when you want to minimize the reconfiguration of hosts on that network.   Figure 5.3 shows an example of a VLAN group.

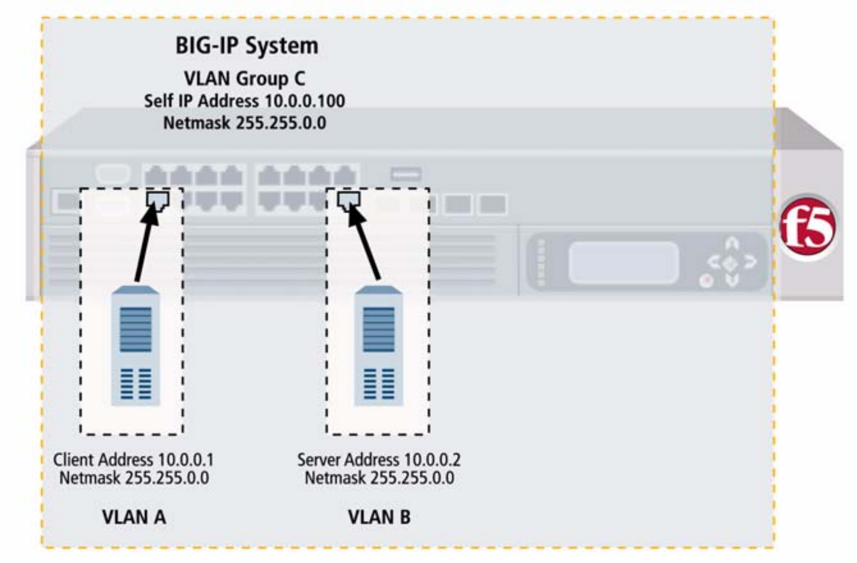


Figure 5.3 *Example of a VLAN group*

A VLAN group also ensures that the BIG-IP system can process traffic successfully between a client and server when the two hosts reside in the same address space. Without a VLAN group, when the client and server both reside in the same address space, the client request goes through the virtual server, but instead of sending its response back through the virtual server, the server attempts to send its response directly to the client, bypassing the virtual server altogether. As a result, the client cannot receive the response, because the client expects the address of the response to be the virtual server IP address, not the server IP address.

Although one way to solve this problem is to enable source network address translation (SNAT), a simpler approach is to create a VLAN group. With a VLAN group, you do not need to translate the client IP address to a different source address. You can preserve the original client IP address, and the server can still send its response to the client successfully.

◆ **Tip**

You can configure the behavior of the BIG-IP system so that it always creates a proxy for any ARP requests between VLANs. For more information, see ***Excluding hosts from proxy ARP forwarding****, on page 5-17.*

When you create a VLAN group, the two existing VLANs become child VLANs of the VLAN group. To create a VLAN group, you use the Configuration utility. For information on managing a VLAN group, see *Managing a VLAN group*, on page 5-17.

Creating a VLAN group

When you create a VLAN group, you assign a name and a VLAN group ID. Then you specify the existing VLANs that you want the VLAN group to contain. Finally, you specify a transparency mode, and some settings related to redundant-system configuration.

◆ **Note**

Two distinct VLANs must exist on the BIG-IP system before you can create a VLAN group.

The settings that you can configure for a VLAN group are summarized in Table 5.2.

Setting	Description	Default Value
Name	Specifies a unique name for the VLAN group. This value is required.	No default value
VLAN Group ID	Specifies an ID for the VLAN group. If you do not specify a VLAN group ID, the BIG-IP system assigns an ID automatically. The value of a VLAN group ID can be between **1** and **4094**.	No default value
VLANs	Specifies the VLANs that you want the VLAN group to contain.	No default value
Transparency Mode	Specifies the level of exposure of remote MAC addresses within a VLAN group. Possible values are: **Opaque**, **Translucent**, and **Transparent**.	**Translucent**
Bridge All Traffic	When enabled (checked), specifies that the VLAN group forwards all frames, including non-IP traffic. The default setting is disabled (unchecked).	Disabled
Bridge in Standby	When enabled (checked), specifies that the VLAN group forwards frames, even when the system is the standby unit in a redundant system. The default setting is enabled (checked).	Enabled
MAC Masquerade	Specifies a MAC masquerade address, used when you have a redundant system.	No default value

Table 5.2 *Configuration options for VLANs*

Use the following procedure to create a VLAN group. For detailed information about each setting, see the sections following the procedure.

◆ **Important**

*In addition to configuring the settings listed in Table 5.2, you must also assign a self IP address to the VLAN group. For more information, see **Assigning self IPs to VLANs and VLAN groups**, on page 5-18.*

To create a VLAN group

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.
2. On the menu bar, from **VLAN Groups,** choose List.
   This displays a list of all existing VLAN groups.
3. In the upper-right corner, click **Create**.
   The VLAN Groups screen opens.
4. In the General Properties area, in the **VLAN Group** box, type a unique name for the VLAN group.
5. In the **VLAN Group ID** box, type a unique VLAN ID.
   If you do not specify a VLAN ID, the BIG-IP system automatically assigns one.
6. In the Configuration area, for the **VLANs** setting, click a VLAN name in the **Available** box, and using the Move button (**<<**), move the VLAN name to the **Members** box.
   Repeat this step as necessary.
7. From the **Transparency Mode** list, select a transparency mode, or use the default setting.
8. Check the **Bridge All Traffic** setting if you want the VLAN group to forward all frames, including non-IP traffic.
9. For the **Bridge in Standby** setting, leave the box checked if you want the VLAN group to forward frames even when the system is the standby unit of a redundant system.
10. In the **MAC Masquerade** box, type a MAC address.
    For more information, see *Specifying a MAC masquerade address*, on page 5-8.
11. Click **Finished**.

Specifying a VLAN group name

When creating a VLAN group, you must assign it a unique name. Once you have finished creating the VLAN group, the VLAN group name appears in the list of existing VLANs groups.

Specifying a VLAN group ID

A ***VLAN group ID*** is a tag for the VLAN group. Every VLAN group needs a unique ID number. If you do not specify an ID for the VLAN group, the BIG-IP system automatically assigns one. The value of a VLAN group ID can be between **1** and **4094**. For more information on VLAN tags, see *Tag-based access to VLANs*, on page 5-6.

Specifying the transparency mode

The BIG-IP system is capable of processing traffic using a combination of layer 2 and layer 3 forwarding, that is, switching and IP routing. When you set the transparency mode, you specify the type of forwarding that the BIG-IP system performs when forwarding a message to a host in a VLAN. The default setting is **translucent**, which means that the BIG-IP system uses a mix of Layer 2 and Layer 3 processing. Table 5.3 lists the allowed values.

Value	Description
opaque	A proxy ARP with layer 3 forwarding.
translucent	Layer 2 forwarding with a locally-unique bit, toggled in ARP response across VLANs. This is the default setting.
transparent	Layer 2 forwarding with the original MAC address of the remote system preserved across VLANs.

Table 5.3 *Modes for VLAN group forwarding*

Bridging all traffic

When you enable this option, you are instructing the VLAN group to forward all non-IP traffic. Note that IP traffic is bridged by default. The default value for this setting is disabled (unchecked).

Bridging traffic with standby units

When this option is enabled (checked), specifies that the VLAN group forwards frames, even when the system is the standby unit in a redundant system.

◆ **WARNING**

This setting can cause adverse effects if the VLAN group exists on both units of the redundant system. The setting is intended for configurations where the VLAN group exists on one unit only. The default setting is enabled (checked).

Specifying a MAC masquerade address

When you place VLANs into a VLAN group, devices on the network automatically send responses to the MAC masquerade address that you assigned to the VLAN group. In this case, the BIG-IP system ignores the MAC masquerade addresses that you assigned to the individual VLANs of the group.

The procedure for assigning a MAC masquerade address to a VLAN group is similar to the procedure for assigning one to a VLAN. However, because interfaces are not assigned directly to a VLAN group, you can use the MAC address of the lowest-numbered interface *of any VLAN in the VLAN group* when you decide on a MAC masquerade address for the VLAN group.

For more information on MAC masquerade addresses, see *Specifying a MAC masquerade address*, on page 5-8.

Managing a VLAN group

Using the Configuration utility, you can change the properties of a VLAN group, delete the VLAN group, or manage the way that the VLAN group handles proxy ARP forwarding.

Changing VLAN group properties

Using the Configuration utility, you can modify all of the properties of a VLAN group, except the VLAN name and VLAN group ID.

To change the properties of a VLAN group

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of existing VLANs.
2. From the **VLAN Groups** menu, choose List.
   This shows a list of existing VLAN groups.
3. Click a VLAN group name.
4. Change the value of any settings.
5. Click **Update**.

Excluding hosts from proxy ARP forwarding

As described earlier, a host in a VLAN cannot normally communicate to a host in another VLAN. This rule applies to ARP requests as well. However, if you put the VLANs into a single VLAN group, the BIG-IP system can perform a proxied ARP request.

A ***proxied ARP request*** is an ARP request that the BIG-IP system can send, on behalf of a host in a VLAN, to hosts in another VLAN. A proxied ARP request requires that both VLANs belong to the same VLAN group.

In some cases, you might not want a host to forward proxied ARP requests to a specific host, such as an active unit in a redundant system that forwards a proxied ARP request to the standby unit, or to other hosts in the configuration. To exclude specific hosts from receiving forwarded proxied ARP requests, you use the Configuration utility and specify the IP addresses that you want to exclude.

◆ **WARNING**

Although hosts on an ARP exclusion list are specified using their IP addresses, this does not prevent the BIG-IP system from routing traffic to those hosts. A more secure way to prevent traffic from passing between hosts in separate VLANs is to create a packet filter for each VLAN.

To exclude the forwarding of proxied ARP requests

1. On the Main tab of the navigation pane, expand **Network** and click **VLANs**.
   This displays a list of all existing VLANs.
2. On the menu bar, from **VLAN Groups**, choose Proxy Exclusion List.
   This opens the Global Proxy Exclusion List screen.
3. In the upper-right corner, click **Create**.
4. In the IP address box, type an IP address that you want to exclude from a proxied ARP request.
5. Click **Repeat** if you want to type another IP address, or click **Finished**.

Assigning self IPs to VLANs and VLAN groups

After you create a VLAN or a VLAN group, you must assign it a self IP address. You assign self IP addresses to VLANs and VLAN groups using the Configuration utility.

- **Assigning a self IP address to a VLAN**
  The self IP address that you assign to a VLAN should represent an address space that includes the self IP addresses of the hosts that the VLAN contains. For example, if the address of one host is **11.0.0.1** and the address of the other host is **11.0.0.2**, you could assign an address of **11.0.0.100**, with a netmask of **255.255.255.0**, to the VLAN.
- **Assigning a self IP address to the VLAN group**
  The self IP address that you assign to a VLAN group should represent an address space that includes the self IP addresses of the VLANs that you assigned to the group. For example, if the address of one VLAN is

10.0.0.1 and the address of the other VLAN is **10.0.0.2**, you could assign an address of **10.0.0.100**, with a netmask of **255.255.255.0**, to the VLAN group.

For more detailed information and the procedure for assigning self IP addresses, see Chapter 6, *Configuring Self IP Addresses*.

6

Configuring Self IP Addresses

- Introducing self IP addresses
- Creating and managing self IP addresses

Introducing self IP addresses

A ***self IP address*** is an IP address that you associate with a VLAN, to access hosts in that VLAN. By virtue of its netmask, a self IP address represents an ***address space***, that is, a range of IP addresses spanning the hosts in the VLAN, rather than a single host address. You can associate self IP addresses not only with VLANs, but also with VLAN groups.

Self IP addresses serve two purposes. First, when sending a message to a destination server, the BIG-IP system uses the self IP addresses of its VLANs to determine the specific VLAN in which a destination server resides. For example, if VLAN **internal** has a self IP address of **10.10.10.100**, with a netmask of **255.255.255.0**, and the destination server's IP address is **10.10.10.20** (with a netmask of **255.255.255.255**), the BIG-IP system recognizes that the server's IP address falls within the range of VLAN **internal**'s self IP address, and therefore sends the message to that VLAN. More specifically, the BIG-IP system sends the message to the interface that you assigned to that VLAN. If more than one interface is assigned to the VLAN, the BIG-IP system takes additional steps to determine the correct interface, such as checking the layer2 forwarding table.

Second, a self IP address serves as the default route for each destination server in the corresponding VLAN. In this case, the self IP address of a VLAN appears as the destination IP address in the packet header when the server sends a response to the BIG-IP system. For more information on configuring the default route of a destination server, see Chapter 13, *Setting up a Redundant System*.

You normally assign self IP addresses to a VLAN when you initially run the Setup utility on a BIG-IP system. More specifically, you assign one static self IP address and one floating self IP address to each of the default VLANs (**internal** and **external**). Later, using the Configuration utility, you can create self IP addresses for other VLANs that you create.

Types of self IP addresses

There are two types of self IP addresses that you can create:

- A ***static self IP address*** is an IP address that the BIG-IP system does not share with another BIG-IP system. By default, the self IP addresses that you create with the Configuration utility are static self IP addresses.
- A ***floating self IP address*** is an IP address that two BIG-IP systems share, such as two units of a redundant system. When you use the Configuration utility to create a self IP address, you can specify that you want the IP address to be floating address.

For more information on static and floating IP addresses, see Chapter 13, *Setting up a Redundant System*.

Self IP addresses and MAC addresses

For each self IP address that you create for a VLAN, the BIG-IP system automatically assigns a media access control (MAC) address. By default, the BIG-IP system assigns the same MAC address that is assigned to the lowest-numbered interface of the VLAN.

As an alternative, you can globally configure the BIG-IP system to assign the same MAC address to all VLANs. This feature is useful if your network includes a type of switch that does not keep a separate layer 2 forwarding table for each VLAN on that switch.

Using self IP addresses for SNATs

When you configure the BIG-IP system to manage local area traffic, you can implement a feature known as a secure network address translation (SNAT). A ***SNAT*** is an object that causes the BIG-IP system to translate the original source IP address of a packet to an IP address that you specify. A SNAT ensures that the target server sends its response back through the BIG-IP system rather than to the original client IP address directly.

When you create a SNAT, you can configure the BIG-IP system to automatically choose a translation address. This ability of the BIG-IP system to automatically choose a translation address is known as ***SNAT automapping***, and in this case, the translation address that the system chooses is always an existing self IP address. Thus, for traffic going from the BIG-IP system to a destination server, configuring SNAT automapping ensures that the source IP address in the header of a packet is a self IP address.

When you create an automapped SNAT, the BIG-IP system actually creates a SNAT pool consisting of the system's internal self IP addresses, and then uses an algorithm to select and assign an address from that SNAT pool.

For more information on SNAT automapping, see the ***Configuration Guide for Local Traffic Management***.

Creating and managing self IP addresses

As stated previously, it is when you initially run the Setup utility on a BIG-IP system that you normally create any static and floating self IP addresses and assign them to VLANs. However, if you want to create additional self IP addresses later, you can do so using the Configuration utility.

Creating a self IP address

The BIG-IP system offers several settings that you can configure for a self IP address. These settings are summarized in Table 6.1.

Setting	Description	Default Value
IP Address	Specifies a self IP address.	No default value
Netmask	Specifies the netmask for the self IP address.	No default value
VLAN	Specifies the VLAN to which this self IP address corresponds.	No default value
Port Lockdown	Specifies the protocols and services from which the self IP address can accept traffic.	**Allow Default**
Floating IP	Specifies that the self IP address is a floating IP address (shared between two BIG-IP systems).	Unchecked

Table 6.1 *Configuration settings for a self IP address*

Use the following procedure to create a self IP address. For detailed information about each setting, see the sections following the procedure.

◆ **Note**

A self IP address can be in either IPv4 or IPv6 format.

To create a self IP address

1. On the Main tab of the navigation pane, expand **Network**, and click **Self IPs**.
   This displays a list of existing self IP addresses.
2. In the upper-right corner of the screen, click the **Create** button.
3. In the **IP Address** box, type the self IP address that you want to assign to a VLAN.
4. In the **Netmask** box, type a netmask.
5. For the **VLAN** setting, select the name of the VLAN to which you want to assign the self IP address.
   The default value is **internal**.

6. For the **Port Lockdown** setting, select **Allow Default**, **Allow All**, **Allow None**, or **Allow Custom**.
   Selecting **Allow Custom** displays the **Custom List** setting. For more information on these setting values, see *Specifying port lockdown*, on page 6-5.
7. If you chose **Allow Custom** in step 7, click **TCP**, **UDP**, or **Protocol**.

   a) If you chose **TCP** or **UDP**, do one or both of the following:

   - Click **All** or **None** and then click **Add**.
     The value **All** or **None** appears in the **TCP** or **UDP** box.
   - Click **Port**, type a port number, and then click **Add**.
     The port number appears in the **TCP** or **UDP** box.

   b) If you chose **Protocol**, select a protocol name and click **Add**.
8. If you want to configure the self IP address as a floating IP address, check the **Floating IP** box.
9. To finish the configuration of this self IP address and create other self IP addresses, click **Repeat** and perform all previous steps until all self IP addresses have been created.
10. Click **Finished**.

Specifying an IP address

As described in *Introducing self IP addresses*, on page 6-1, a self IP address, combined with a netmask, typically represents a range of host IP addresses in a VLAN. If you are assigning a self IP address to a VLAN group, the self IP address represents the range of self IP addresses assigned to the VLANs in that group.

The self IP address that you specify in the **IP Address** setting is a static IP address, unless you enable the **Floating IP** setting. For more information, see *Specifying a floating IP address*, on page 6-5.

Specifying a netmask

When you specify a netmask for a self IP address, the self IP address can represent a range of IP addresses, rather than a single host address. For example, a self IP address of **10.0.0.100** can represent several host IP addresses if you specify a netmask of **255.255.0.0**.

Associating a self IP address with a VLAN

You assign a unique self IP address to a specific VLAN or a VLAN group:

- **Assigning a self IP address to a VLAN**
  The self IP address that you assign to a VLAN should represent an address space that includes the self IP addresses of the hosts that the VLAN contains. For example, if the address of one destination server in

a VLAN is **10.0.0.1** and the address of another server in the VLAN is **10.0.0.2**, you could assign a self IP address of **11.0.0.100**, with a netmask of **255.255.0.0**, to the VLAN.

- **Assigning a self IP address to a VLAN group**
  The self IP address that you assign to a VLAN group should represent an address space that includes the self IP addresses of the VLANs that you assigned to the group. For example, if the self IP address of one VLAN in a VLAN group is **10.0.20.100** and the address of the other VLAN in a VLAN group is **10.0.30.100**,you could assign an address of **10.0.0.100**, with a netmask of **255.255.0.0**, to the VLAN group.

The **VLAN** list displays the names of all existing VLANs and VLAN groups.

Specifying port lockdown

Each self IP address has a feature known as port lockdown. ***Port lockdown*** is a security feature that allows you to specify particular UDP and TCP protocols and services from which the self IP address can accept traffic. By default, a self IP address accepts traffic from these protocols and services:

- For UDP, the allowed protocols and services are: DNS (53), SNMP (161), RIP (520)
- For TCP, the allowed protocols and services are: SSH (22), DNS (53), SNMP (161), HTTPS (443), 4353 (iQuery)

If you do not want to use the default setting (**Allow Default**), you can configure port lockdown to allow either all UDP and TCP protocols and services (**Allow All**), no UDP protocols and services (**Allow None**), or only those that you specify (**Allow Custom**).

Specifying a floating IP address

You can enable the **Floating IP** setting if you want the self IP address to be a floating IP address, that is, an address shared between two BIG-IP systems. A floating self IP address enables a destination server to successfully send a response when the relevant BIG-IP unit is unavailable. When two units share a floating self IP address, a destination server can send traffic to that address instead of a static self IP address. If the target unit is unavailable, the peer unit can receive and process that traffic. Without this shared floating IP address, the delivery of server traffic to a unit of a redundant system can fail.

◆ **Note**

*The **Floating IP** setting appears on the screen only when the BIG-IP system is configured as a unit of a redundant system. For more information on configuring a redundant system, see Chapter 13, **Setting up a Redundant System**.*

Managing self IP addresses

Using the Configuration utility, you can view or change the properties of a self IP address, or delete a self IP address.

To view or modify the settings of a self IP address

1. On the Main tab of the navigation pane, expand **Network**, and click **Self IPs**.
   This displays a list of existing self IP addresses.
2. In the IP Address column, click a self IP address.
   This displays the properties page for that self IP address.
3. To change the setting values, modify the values and click **Update**.
   This displays the list of existing self IP addresses.

◆ **Note**

*You can modify any setting except **IP Address.** To modify the **IP Address** setting, you must delete the self IP address and create a new one. For more information, see **To delete a self IP address**, following, and **To create a self IP address**, on page 6-3.*

To delete a self IP address

1. On the Main tab of the navigation pane, expand **Network**, and click **Self IPs**.
   This displays a list of existing self IP addresses.
2. In the IP address column, locate the self IP address you want to delete.
3. Click the select box to the left of the IP address.
4. Click **Delete**.
   A confirmation screen appears.
5. Click **Delete**.

7

Working with Interfaces

- Introducing BIG-IP system interfaces
- Configuring interfaces
- Configuring interface mirroring
- Displaying interface statistics
- Related configuration tasks

Introducing BIG-IP system interfaces

A key task of the BIG-IP system configuration is the configuration of BIG-IP system interfaces. The ***interfaces*** on a BIG-IP system are the physical ports that you use to connect the BIG-IP system to other devices on the network. These other devices can be next-hop routers, layer 2 devices, destination servers, and so on. Through its interfaces, the BIG-IP system can forward traffic to or from other network devices.

◆ **Note**

*Throughout this guide, the term **interface** refers to the physical ports on the BIG-IP system.*

Every BIG-IP system includes multiple interfaces. The exact number of interfaces that you have on the BIG-IP system depends on the platform type. For information on BIG-IP platform types, see ***Platform Guide: 1500, 3400, 6400, and 6800***.

One of the interfaces on the BIG-IP system is a special interface dedicated to performing a specific set of system management functions. This interface is called the ***management interface***, named **MGMT**. All other interfaces on the BIG-IP system are known as TMM switch interfaces. ***TMM switch interfaces*** are those interfaces that the BIG-IP system uses to send or receive application traffic, that is, traffic slated for load balancing. The remainder of this chapter describes how to configure TMM switch interfaces. For information on how to configure and use the management interface, see Chapter 4, *Configuring the BIG-IP Platform and General Properties*.

Each of the interfaces on the BIG-IP system has unique properties, such as media speed, duplex mode, VLAN tagging, and spanning tree protocol settings. You can use the Configuration utility to configure these properties. For more information, see *Configuring interfaces*, on page 7-2.

In addition to configuring interface properties, you can implement a feature known as interface mirroring, which you can use to duplicate traffic from one or more interfaces to another. You can also view statistics about the traffic on each interface. For more information, see *Configuring interface mirroring*, on page 7-6 and *Displaying interface statistics*, on page 7-7.

Once you have configured the properties of each interface, you can configure several other features of the BIG-IP system that control the way that interfaces operate. For example, by creating a virtual local area network (VLAN) and assigning interfaces to it, the BIG-IP system can insert a VLAN ID, or ***tag***, into frames passing through those interfaces. In this way, a single interface can forward traffic for multiple VLANs. For more information on configuring other BIG-IP features related to interfaces, see *Related configuration tasks*, on page 7-9.

Configuring interfaces

Each interface on the BIG-IP system has a set of properties that you can configure, such as enabling or disabling the interface, setting the requested media type and duplex mode, and configuring flow control. Configuring the properties of each interface is one of the first tasks you do after running the Setup utility on the BIG-IP system. While you can change some of these properties, such as media speed and duplex mode, you cannot change other properties, such as the media access control (MAC) address.

◆ **Note**

*For information on configuring STP-related properties on an interface, see Chapter 12, **Configuring Spanning Tree Protocols**.*

Before configuring interface properties, it is helpful to understand interface naming conventions.

Understanding interface naming conventions

By convention, the names of the interfaces on the BIG-IP system use the format **<s>.<p>** where **s** is the slot number of the network interface card (NIC), and **p** is the port number on the NIC. Examples of interface names are 1.1, 1.2, and 2.1. BIG-IP system interfaces already have names assigned to them; you do not explicitly assign them.

An exception to the interface naming convention is the management interface, which has the special name MGMT. For more information on the management interface, see Chapter 4, *Configuring the BIG-IP Platform and General Properties*.

Viewing interface information and media properties

Using the Configuration utility, you can display a screen that lists all of the BIG-IP system interfaces, as well as their current status (**UP** or **DOWN**). You can also view other information about each interface:

- The MAC address of the interface
- The media type and duplex mode (such as **100baseTX full**)
- The number of VLANs to which the interface is assigned
- A trunk name, if the interface is assigned to a trunk

This information is useful when you want to assess the way that a particular interface is forwarding traffic. For example, you can use this information to determine the specific VLANs for which an interface is currently forwarding traffic. You can also use this information to determine the speed at which an interface is currently operating.

On the General Properties screen for interfaces, you can view the media speed and the duplex mode of an interface. Use the following procedures to view the list of interfaces and related information, and to view the media properties of an interface.

To view a list of interfaces and related information

On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**. This displays a list of the interfaces on the BIG-IP system, along with their status and related information.

To view media properties for an interface

1. On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**.
   This displays the list of the interfaces on the BIG-IP system.
2. Click an interface name in the list.
   This displays the general properties of that interface, as well as some configuration settings.
3. In the General Properties area of the screen, view the **Media Speed** and **Active Duplex** properties.

Configuring interface properties

You can configure a number of general properties for each interface. When you configure these properties, you customize the way that the interface forwards traffic. For example, if you want the interface to operate as part of a trunk, you can set the **Requested Duplex** mode to **full**, which is a requirement for trunk participation. Table 7.1 lists and describes these properties.

Interface Properties	Description	Default Value
State	Enables or disables the interface.	**Enabled**
Requested Media	Specifies a media type and mode, or **auto** for automatic detection.	**auto**
Flow Control	Specifies how an interface handles pause frames for flow control.	**Pause TX/RX**

Table 7.1 *The properties you can configure for an interface*

Use the following procedure to configure the general properties of an interface. For detailed information on these individual properties, see the sections following the procedure.

◆ **Note**

*To configure STP-related settings, see Chapter 12, **Configuring Spanning Tree Protocols**.*

To configure general interface properties

1. On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**.
   This displays the list of the interfaces on the BIG-IP system.
2. In the Name column, click an interface name.
   This displays the general properties of that interface, as well as some configuration settings.
3. In the Configuration area, configure the properties as needed.
   For information on each property, see the following sections.
4. Click **Update**.

Configuring the state of an interface

You can either enable or disable an interface on the BIG-IP system, by configuring the **State** property. By default, each interface is set to **Enabled**, where it can accept ingress or egress traffic. When you set the state to **Disabled**, the interface cannot accept ingress or egress traffic.

Setting the requested media type

You can configure the **Requested Media** property to specify the media type and duplex mode of the interface card, or you can use the **auto** setting for auto-detection. The values that you can choose from when configuring the **Requested Media** property are: **auto**, **10baseT full**, **10baseT half**, **100baseTX full**, **100baseTX half,** and **1000baseT full**, and **1000baseT half**.

The default setting for this property is **auto**. 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 **1000BaseT half**.

Full duplex mode means that traffic on that interface can travel in both directions simultaneously, while ***half duplex*** mode means that traffic on that interface can only travel in one direction at any given time. Note that if you want the interface to be part of a trunk, the media type must be set to one with full duplex mode.

If the media type of the interface does not allow the duplex mode to be set, this is indicated by an on-screen message. If setting the duplex mode is not supported for the interface, the duplex setting is not saved to the **bigip_base.conf** file.

◆ **Note**

If the BIG-IP system is inter-operating with an external switch, the media setting should match that of the external switch.

Configuring flow control

You can configure the **Flow Control** property to manage the way that an interface handles pause frames for flow control. ***Pause frames*** are frames that an interface sends to a peer interface as a way to control frame transmission from that peer interface. Pausing a peer's frame transmissions prevents an interface's First-in, First-out (FIFO) queue from filling up and resulting in a loss of data. Possible values for this property are:

- **Pause None**
  Disables flow control.
- **Pause TX/RX**
  Specifies that the interface honors pause frames from its peer, and also generates pause frames when necessary. This is the default value.
- **Pause TX**
  Specifies that the interface ignores pause frames from its peer, and generates pause frames when necessary.
- **Pause RX**
  Specifies that the interface honors pause frames from its peer, but does not generate pause frames.

Configuring interface mirroring

For reliability reasons, you can configure a feature known as interface mirroring. When you configure ***interface mirroring***, you cause the BIG-IP system to copy the traffic on one or more interfaces to another interface that you specify. By default, the interface mirroring feature is disabled.

The settings you configure to implement the interface mirroring feature are shown in Table 7.2.

Setting	Description
Interface Mirroring State	Enables or disables interface mirroring.
Destination Interface	Specifies the interface on which traffic from other interfaces is to be mirrored.
Mirrored Interfaces	Specifies one or more interfaces for which you want to mirror traffic on the destination interface.

Table 7.2 *Configuration settings for enabling interface mirroring*

Use the following procedure to configure interface mirroring.

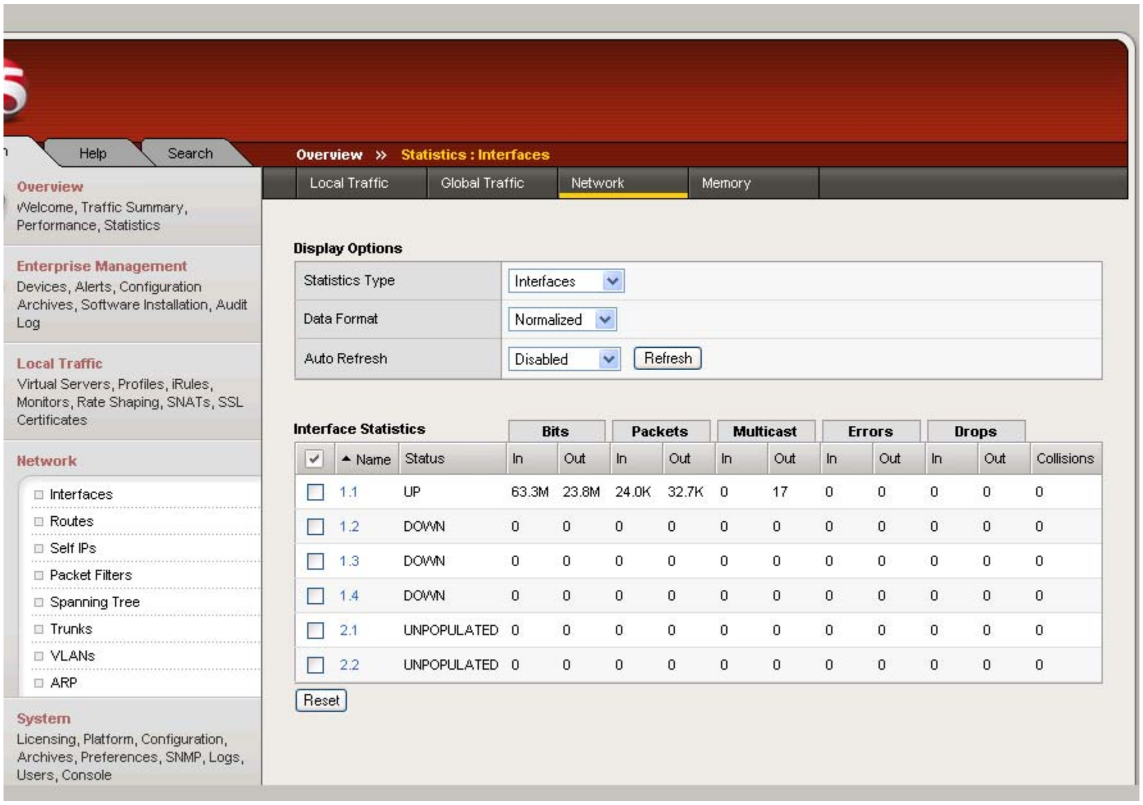
To configure interface mirroring

1. On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**.
   This displays the list of the interfaces on the BIG-IP system.
2. On the menu bar, click **Interface Mirroring**.
   The Interface Mirroring screen opens.
3. From the **Interface Mirroring State** list, select Enabled.
   This displays additional configuration settings.
4. From the **Destination Interface** list, select the interface that you want the BIG-IP system to use for mirrored traffic.
5. For the **Mirrored Interfaces** setting, click an interface number in the **Available** box, and using the Move button (**<<**), move the interface number to the **Selected** box. Repeat this step for each interface that you want to mirror.
6. Click **Update**.

Displaying interface statistics

You can display a variety of statistics about the interfaces on the BIG-IP system. Figure 7.1 shows an example of the output you see when you display interface statistics on an active unit of a redundant system.

.


Help
Search
Overview » Statistics : Interfaces
Local Traffic
Global Traffic
Network
Memory
Overview
Welcome, Traffic Summary, Performance, Statistics
Enterprise Management
Devices, Alerts, Configuration Archives, Software Installation, Audit Log
Local Traffic
Virtual Servers, Profiles, iRules, Monitors, Rate Shaping, SNATs, SSL Certificates
Network
Interfaces
Routes
Self IPs
Packet Filters
Spanning Tree
Trunks
VLANs
ARP
System
Licensing, Platform, Configuration, Archives, Preferences, SNMP, Logs, Users, Console
Refresh
Reset

Display Options

Statistics Type	Interfaces
Data Format	Normalized
Auto Refresh	Disabled

Interface Statistics

			Bits		Packets		Multicast		Errors		Drops		
☑	▲ Name	Status	In	Out	In	Out	In	Out	In	Out	In	Out	Collisions
□	1.1	UP	63.3M	23.8M	24.0K	32.7K	0	17	0	0	0	0	0
□	1.2	DOWN	0	0	0	0	0	0	0	0	0	0	0
□	1.3	DOWN	0	0	0	0	0	0	0	0	0	0	0
□	1.4	DOWN	0	0	0	0	0	0	0	0	0	0	0
□	2.1	UNPOPULATED	0	0	0	0	0	0	0	0	0	0	0
□	2.2	UNPOPULATED	0	0	0	0	0	0	0	0	0	0	0

Figure 7.1 *Sample interface statistics screen*

◆ **Tip**

For descriptions of each type of statistic, see the online help.

To display interface statistics

1. On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**.
   This displays the list of the interfaces on the BIG-IP system.

2. On the menu bar, click **Statistics**.
   This displays statistics for the interfaces on the BIG-IP system.

3. In the Display Options area of the screen, verify that the **Statistics Type** setting is set to **Interfaces**.

4. For the **Data Format** setting, retain the default value (**Normalized**), or select **Unformatted** from the list.
5. For the **Auto Refresh** setting, retain the default value of **Disabled**, or select an automatic refresh interval from the list.

   Note: *Setting the* ***Auto Refresh*** *value to a short interval could impact system performance.*
6. If you want to manually refresh the statistics, click **Refresh**.

Related configuration tasks

After you have configured the interfaces on the BIG-IP system, one of the primary tasks you perform is to assign those interfaces to the virtual LANs (VLANs) that you create. A ***VLAN*** is a logical subset of hosts on a local area network (LAN) that reside in the same IP address space. When you assign multiple interfaces to a single VLAN, traffic destined for a host in that VLAN can travel through any one of these interfaces to reach its destination. Conversely, when you assign a single interface to multiple VLANs, the BIG-IP system can use that single interface for any traffic that is intended for hosts in those VLANs. For more information on VLANs and assigning interfaces to them, see Chapter 5, *Configuring VLANs and VLAN Groups*.

Another powerful feature that you can use for BIG-IP system interfaces is trunking, with link aggregation. A ***trunk*** is an object that logically groups physical interfaces together to increase bandwidth. Link aggregation, through the use of the industry-standard Link Aggregation Control Protocol (LACP), provides regular monitoring of link status, as well as failover if an interface becomes unavailable. For more information on using trunks and LACP, see Chapter 10, *Working with Trunks*.

Finally, you can configure your BIG-IP system interfaces to work with one of the spanning tree protocols (STP, RSTP, and MSTP). ***Spanning tree protocols*** reduce traffic on your internal network by blocking duplicate routes to prevent bridging loops. Chapter 12, *Configuring Spanning Tree Protocols*, describes the spanning tree protocols and the procedure for configuring these protocols on the BIG-IP system. The chapter also includes information on setting spanning tree-related properties on individual interfaces.

8

Configuring Routes

- Introducing route configuration
- Understanding the TMM routing table
- Configuring the TMM routing table
- Considering other routing issues

Introducing route configuration

The BIG-IP system must communicate with other routers, servers, and firewalls in a networked environment. Before you put the BIG-IP system into production, we recommend that you carefully review the router and server configurations in your network. By doing so, you can properly configure routing on the BIG-IP system, and you can adjust the routing configurations on other network devices to include various BIG-IP system IP addresses. Depending on how you configure routing, the BIG-IP system can forward packets to a specified network device (such as a next-hop router or a destination server), or the system can drop packets altogether.

Due to its IP routing (layer 3) capabilities, combined with the need to process both user application traffic (for load balancing) and administrative traffic, the BIG-IP system contains two routing tables. The first is the Linux kernel routing table, which stores and retrieves information about management routes. ***Management routes*** are routes that the BIG-IP system uses to forward traffic through the special management (**MGMT**) interface.

The other routing table is the main TMM routing table, which stores and retrieves IP routing information about TMM switch routes. ***TMM switch routes*** are routes that the BIG-IP system uses to forward traffic through the TMM switch interfaces instead of through the management interface.

Unless noted otherwise, the remainder of this chapter describes how to configure TMM switch routes only. For more information on configuring routes for the management interface, see *Routing traffic through the management interface*, on page 8-11, and Chapter 4, *Configuring the BIG-IP Platform and General Properties*.

Understanding the TMM routing table

The purpose of the TMM routing table is to store essential routing information for traffic passing through the TMM system. The BIG-IP system creates a routing table automatically when you configure its local interfaces. Once the routing table is created, there are two ways to maintain it:

- You can add entries to the routing table, using the Configuration utility. These entries are called ***static entries***.
- You can use one or more dynamic routing protocols to automatically update the routing table on a regular basis. These entries are called ***dynamic entries***.

Typically, a routing table on the BIG-IP system contains a combination of static and dynamic entries. The remainder of this section describes how to add and maintain static entries.

You can use the Configuration utility to add static routes to the TMM routing table. When you add an entry to the routing table, you specify a destination host or network, and a gateway through which traffic for that destination should pass to reach the destination address. You can also add an entry for a default route.

On a typical router, you define the gateway for each route as the address for a next-hop router. On the BIG-IP system, however, the gateway that you specify can be any of four different ***resource types***: A next-hop router address, the name of a pool of routers, a VLAN name, or an instruction to reject the packet.

- ◆ **A next-hop router address**
  A next-hop router address is also known as a gateway address. A ***gateway address*** specifies a particular router that the BIG-IP system should use when forwarding packets to the destination host or network.
- ◆ **A name of a pool of routers**
  Rather than specifying a specific next-hop router, you can specify an entire pool of routers. When you specify this resource type, the BIG-IP system load balances the packets twice, once to a router in the pool of routers, and again to a server in the load balancing pool. Just as with a load balancing pool, the BIG-IP system uses the Round Robin load balancing method by default when forwarding packets to a pool of routers.
- ◆ **A VLAN name**
  Specifying a VLAN name indicates that the network you specify as a destination in a route entry is directly connected to the BIG-IP system. Therefore, the BIG-IP system can send an ARP request to any host in that network to obtain the MAC address of the destination host.
- ◆ **Reject**
  Setting the resource type to **Reject** causes the BIG-IP system to drop packets that are destined for the specified destination IP address.

Configuring the TMM routing table

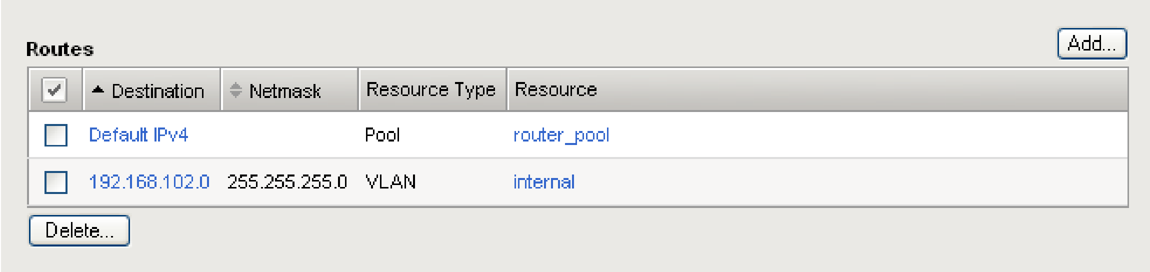
Using the Configuration utility, you can easily manage the static routes defined in the BIG-IP system's TMM routing table. Specifically, you can:

- View static route entries in the routing table
- Add new static route entries to the routing table
- Modify static route entries in the routing table
- Delete static route entries from the routing table that no longer apply due to changes in the network

For information on configuring routes for the management interface, see Chapter 4, *Configuring the BIG-IP Platform and General Properties*.

Viewing the list of static entries

Using the Configuration utility, you can view the list of static entries that you have added to the routing table. Figure 8.1 shows an example of a list containing two static entries. The first entry shows a default route that uses a pool of routers as the resource. The second entry shows a route to a destination host, where the route uses a VLAN as the resource.



☑	▲ Destination	⇕ Netmask	Resource Type	Resource
□	Default IPv4		Pool	router_pool
□	192.168.102.0	255.255.255.0	VLAN	internal

Figure 8.1 *A sample list of static routes*

When you view the list of entries, you can see the following information:

- **The destination IP address**
  For the destination address, you can see either a default entry, a host destination, or a network address.
- **The netmask**
  This is the netmask of the destination address. No netmask appears for the default route.
- **The resource type**
  The resource type appears as either Gateway, Pool, VLAN, or Reject.
- **The resource name**
  The resource name is either a next-hop-router (gateway) address, a pool name, or a VLAN name.

To view a list of static entries

On the Main tab of the navigation pane, expand **Network** and click **Routes**. The Configuration utility displays the list of static entries.

◆ **Tip**

You can also view static TMM route entries by displaying a section of the ***/config/bigip.conf*** *file, using the* ***bigpipe*** *command line utility. Simply type the command* ***bigpipe route list all*** *at a command line prompt.*

Adding static entries to the TMM routing table

You use the Configuration utility to add static entries to the TMM routing table. A static entry that you add can be either the default TMM route or a non-default TMM route.

◆ **Important**

We highly recommend that you define a default TMM route. Otherwise, certain types of administrative traffic that would normally use a TMM switch interface might instead use the management interface.

Use the following procedure to add an entry to the TMM routing table. For more detailed information, see Table 8.1, on page 8-5, as well as the sections that follow that table.

◆ **Important**

Before specifying a pool of routers as a gateway, verify that you have created the pool.

For information on verifying the existence of pool, see **To verify the existence of a pool of routers**, on page 8-8. Before specifying a VLAN as a gateway, verify that you have created the VLAN. For more information, see **To verify the existence of a VLAN**, on page 8-9.

To add a static route

1. On the Main tab of the navigation pane, expand **Network**, and click **Routes**.
   The Routes screen opens.
2. On the upper-right corner of the screen, click **Add**.
3. From the **Type** list, select **Default Gateway** or **Route**.

   Note: *Selecting* ***Default Gateway*** *disables the* ***Destination*** *and* ***Netmask*** *properties.*
4. If you selected **Route** in the previous step, specify two settings:

   a) In the **Destination** box, type a destination IP address.

   b) In the **Netmask** box, type the netmask for the IP address you typed in the **Destination** box.
5. For the **Resource** property, select a resource from the list.
   For detailed information on resources, see *Specifying a resource*, on page 8-7.
6. Click **Finished**.

Table 8.1 lists and describes the properties that you configure when adding routing table entries. For detailed information on each property, see the sections that follow the table. For background information on static routing-table entries, see *Understanding the TMM routing table*, on page 8-2.

Property	Description	Default Value
Type	Specifies the routing table entry as either a default route or a standard destination address. Possible values are **Default Gateway** and **Route**.	**Default Gateway**
Destination	Specifies an IP address for the Destination column of the routing table. You can only configure this property when you set the **Type** property to **Route**. When the **Type** property is set to **Default Gateway**, the destination is always shown in the routing table as **0.0.0.0**.	**0.0.0.0** (when **Type** is **Default Gateway**) No default value (when **Type** is **Route**)

Table 8.1 *Configuration properties for adding entries to the routing table*

Property	Description	Default Value
Netmask	Specifies the netmask for a destination address. This value appears in the Genmask column of the routing table. You can only configure this property when you set the **Type** property to **Route**. When the **Type** property is set to **Default Gateway**, the netmask is always shown in the routing table as **0.0.0.0**.	**0.0.0.0** (when **Type** is **Default Gateway**) No default value (when **Type** is **Route**)
Resource	Specifies the particular gateway IP address, pool, or VLAN that the BIG-IP system should use to forward a packet to the destination. Possible values are: **Use Gateway**, **Use Pool**, **Use VLAN**, or **Reject**. Note that you typically select **Use VLAN** for non-default routes only.	**Use Gateway**

Table 8.1 *Configuration properties for adding entries to the routing table*

Specifying a static route type

You use the **Type** property to specify the type of static route that you want to define in the routing table. A static route that you add to the TMM routing table can be either of two types: a non-default route or a default route. On the screen for creating a static route entry, a non-default route is simply called a *route*. A default entry is called a *default gateway*.

You add a route when you want to provide a route that either corresponds directly to the destination IP address of a packet, or specifies the network portion of the destination IP address of a packet.

You add a default gateway when you want to provide the route that the BIG-IP system should use for forwarding packets when no other entry in the routing table matches the destination IP address of the packet.

◆ **Important**

*The information in this section pertains to the default route for the TMM routing table only, and not for the default management route. For information on configuring the default management route, see **Routing traffic through the management interface**, on page 8-11, and Chapter 4, **Configuring the BIG-IP Platform and General Properties**.*

Specifying a destination IP address

When you want to define a non-default route, you use the **Destination** property. If you are defining a default route, this property is unavailable.

Using the **Destination** property, you can specify either a specific destination IP address, to match the destination IP address of a packet, or the network portion of a destination IP address of a packet.

For example, if you want the BIG-IP system to be able to forward packets destined for IP address **192.168.16.240**, you could specify one of the following addresses:

- **192.168.16.240**
  In this case, the BIG-IP system forwards any packet with the exact destination IP address of **192.168.16.240** to the gateway that you define in that routing table entry.

- **192.168.16.0**
  In this case, the BIG-IP system forwards to the gateway any packets with a destination IP address that includes the network ID **192.168.16**.

◆ **Note**

*For information on defining a gateway, see **Specifying a netmask**, following.*

Specifying a netmask

You use the **Netmask** property when you want to define a non-default route. If you are defining a default route, this property is unavailable.

Using the **Netmask** property, you specify the netmask for the destination IP address that you defined with the **Destination** property. The purpose of the netmask is to indicate whether the IP address defined in the **Destination** property is a host address or a network address.

Specifying a resource

Any entry that you add to the TMM routing table includes either a next-hop router, a pool of routers, or a VLAN as the gateway, or ***resource***, through which to send traffic. To specify a resource in a routing table entry, you use the **Resource** property. You can also instruct the BIG-IP system to reject packets for the specified destination IP address.

Figure 8.2 shows part of a sample **bigip.conf** file that results when you specify a pool of routers, a next-hop router, or a VLAN as a resource. The figure also shows an entry that results when you want the system to reject packets destined for a particular host or network.

```
route default inet {
   vlan none
   gateway none
   pool router_pool                             # Resource is a pool of routers
   mtu 0
}
route 192.168.102.0 netmask 255.255.255.0 {
   vlan none
   gateway 192.168.104.101                      # Resource is a next-hop router
   pool none
   mtu 0
}
route 192.168.200.0 netmask 255.255.255.0 {
   vlan internal                                # Resource is a VLAN
   gateway none
   pool none
   mtu 0
}
route 192.168.240.0 netmask 255.255.255.0 {
   reject                                     # Packets dropped for destination network
   vlan none
   gateway none
   pool none
   mtu 0
}
```

Figure 8.2 *Portion of a sample* ***bigip.conf*** *file*

Specifying a pool of routers

A common scenario when adding a route is to define the gateway as a pool of routers instead of a single next-hop router. For example, you can create a pool named **router_pool**, and specify the pool as the gateway for the default route. You can see this route in the first entry of Figure 8.2.

Before you specify a pool of routers as a gateway in the routing table, however, you must create the pool, using the same Configuration utility screens that you use for creating a pool of load balancing servers.

For more information on creating a pool, see the ***Configuration Guide for Local Traffic Management***. For background information on using a pool of routers as a gateway, see *Understanding the TMM routing table*, on page 8-2.

To verify the existence of a pool of routers

On the Main tab of the navigation pane, expand **Local Traffic**, and click **Pools**. This displays the list of existing pools on the BIG-IP system. This list includes any load balancing pools and router pools that you have created.

Specifying a next-hop router

If you know that a server in a load balancing pool is on the same internal network as the BIG-IP system's next-hop router, you can add an entry that defines the server's IP address as the destination, and the next-hop router address as the gateway. For example, the second route entry in Figure 8.2 shows a destination network address of **192.168.102.0**, and a next-hop router address of **192.168.104.101**.

Specifying a VLAN

The gateway address in a routing entry can also be a VLAN name. You can select a VLAN name as a resource when the destination address you specify in the routing entry is a network address. Using a VLAN name as a resource implies that the specified network is directly connected to the BIG-IP system. In this case, the BIG-IP system can find the destination host simply by sending an ARP request to the hosts in the specified VLAN, thereby obtaining the destination host's MAC address. Then, the BIG-IP system simply checks the VLAN's layer 2 forwarding table to determine the correct interface through which to forward the packet.

To verify the existence of a VLAN

On the Main tab of the navigation pane, expand **Network**, and click VLANs. This displays the list of existing VLANs on the BIG-IP system.

Specifying packet rejection

Sometimes, you might want the BIG-IP system to drop any packets destined for the IP address specified as the destination in a routing entry. In this case, you simply select **Reject** as the value for the **Resource** setting when creating a route entry.

Modifying static entries in the routing table

For a static entry in the routing table, you can modify the resource that you specified when you added the entry. You cannot modify the entry type (**Default Gateway** or **Route**), the destination address, or the netmask.

◆ **Important**

Before specifying a pool of routers as a gateway, verify that you have created the pool.

For information on verifying the existence of a pool, see **To verify the existence of a pool of routers**, on page 8-8. Before specifying a VLAN as a gateway, verify that you have created the VLAN. For more information, see *To verify the existence of a VLAN*, on this page.

To modify the resource for an entry

1. On the Main tab of the navigation pane, expand **Network**, and click **Routes**.
   This displays the list of static routes.
2. In the Destination column, click an entry.
3. For the **Resource** property, select a resource from the list.
   For detailed information on resources, see *Specifying a resource*, on page 8-7.
4. Click **Update**.

Deleting static entries from the routing table

Deleting entries from the routing table is necessary when the routers or destination hosts on your network change for any reason. For example, you might remove a specific host or router from the network, thereby invalidating a destination or gateway address in the routing table. You can easily delete static entries using the Configuration utility.

To delete a route

1. On the Main tab of the navigation pane, expand **Network** and click **Routes**.
   A list of the static entries in the routing table appears.
2. Click the Select box to the left of the entry you want to delete.
3. Click **Delete**.
   A confirmation message appears.
4. Click **Delete**.

Considering other routing issues

After you have configured the TMM routing table on the BIG-IP system, you might want to consider some other routing issues. For example, it is customary to ensure that the routers on the network have information about the various IP addresses for the BIG-IP system, such as virtual server addresses, self IP addresses for VLANs, and so on. Fortunately, the BIG-IP system eases this task by sending gratuitous Address Resolution Protocol (ARP) messages to other routers on the network, to notify them of BIG-IP system IP addresses. For more information on ARP and the BIG-IP system, see Chapter 9, *Configuring Address Resolution Protocol*.

You should also consider the following:

- Dynamic routing, using ZebOS routing modules
- The routes for the management interface
- The default route on destination servers

Configuring dynamic routing

The beginning of this chapter explained that there are two types of entries in the BIG-IP system routing table: static entries and dynamic entries. The chapter then described how to add and delete static entries. If you want the system to add entries dynamically, you can use one of the ZebOS routing modules.

Routing traffic through the management interface

When configuring routes on a BIG-IP system, it is helpful to understand the differences between management routes and TMM routes. This is because there are certain administrative tasks, such as a system installation, that you should perform only when the TMM is not running. In those cases, the BIG-IP system uses the default management route for processing that traffic.

We recommend that you read the guide ***Installation, Licensing, and Upgrades for BIG-IP® Systems***. for procedures on configuring the management interface. You should also read the section in Chapter 4, *Configuring the BIG-IP Platform and General Properties*, that describes the management interface. Chapter 18, *Configuring BIG-IP System Services*, suggests some of the administrative tasks that you should perform only when the TMM service is stopped.

Finally, make sure that you have defined a default TMM route in the main TMM routing table. Defining a default TMM route prevents high volumes of administrative traffic generated by the BIG-IP system from using the management interface. For more information, see *Adding static entries to the TMM routing table*, on page 8-4.

Configuring the default route on destination servers

Part of managing routes on a network is making sure that destination servers on the network can route responses to the BIG-IP system. To do this, you should configure the default route on each load balancing server to forward responses to the BIG-IP system.

Configuring the default route on your destination servers is a typical network configuration task. A primary reason for configuring the default route on each server to forward responses to the BIG-IP system is to avoid interruption of service if you have a redundant system configuration and an active unit becomes unavailable. In this case, you want the default route entry on the servers in your load balancing pools to specify a floating self IP address that the two units of the redundant system share. By setting the default route of your destination servers to a floating self IP address, you ensure that if one unit becomes unavailable for any reason, the other unit can still process the responses.

To configure the default route on your destination servers, see the product documentation from your server vendor.

For more information on configuring a redundant system, see Chapter 13, *Setting up a Redundant System*.

9

Configuring Address Resolution Protocol

- Introducing Address Resolution Protocol
- Configuring static entries in the ARP cache
- Configuring dynamic entries in the ARP cache

Introducing Address Resolution Protocol

The BIG-IP system is a multilayer network device, and as such, needs to perform routing functions. To do this, the BIG-IP system must be able to find destination MAC addresses on the network, based on known IP addresses. The way that the BIG-IP system does this is by supporting Address Resolution Protocol (ARP), an industry-standard layer 3 protocol.

What is ARP?

ARP is a protocol that sends a broadcast request to other devices on the network, asking for a destination layer 2 address. Such a request consists of special packets commonly known as who-has packets. ***Who-has*** packets are packets that the BIG-IP system broadcasts to all devices on a network (or VLAN), to determine the owner of a specific IP address. The device owning that IP address typically responds with an ARP packet that contains both its IP address and its MAC address. After receiving an ARP response, the BIG-IP system then stores that device's MAC address in its ARP cache for later use. The ***ARP cache*** is a repository of IP address/MAC address pairs for hosts on a network.

◆ **Note**

Except when referring to the BIG-IP system, the terms ***device****,* ***host****,* ***destination****, or* ***destination address*** *refer to either a destination server or a next-hop router.*

The ARP cache can consist of two types of entries:

- **Static**
  A ***static*** entry is an IP address/MAC address pair that you explicitly add to the ARP cache because you already know the MAC address of a given IP address.
- **Dynamic**
  A ***dynamic*** entry is an IP address/MAC address pair that the BIG-IP system adds to the ARP cache automatically after receiving a response from an ARP broadcast request.

You can use the Configuration utility to manage static and dynamic entries in the ARP cache of the BIG-IP system. When you manage the entries in the ARP cache, you maximize the chance that the BIG-IP system can forward packets to destination hosts successfully and efficiently.

Managing static entries refers to adding IP address/MAC address pairs to the ARP cache, as well as viewing, modifying, or deleting them.

Managing dynamic entries primarily refers to configuring a set of global options that affect the way that the BIG-IP system treats dynamic entries. For example, with the **Dynamic Timeout** option, you can specify the length of time that dynamic entries remain in the ARP cache. With the **Request Retries** option, you can specify the maximum number of times that the

BIG-IP system can send the same ARP request before declaring a destination host to be unreachable. You can view or delete dynamic entries, but you cannot add or modify them.

How does the BIG-IP system use ARP?

When the BIG-IP system needs to forward packets to a destination host or next-hop router, the system starts by searching its ARP cache for the destination IP address and its corresponding MAC address.

If an entry for the IP address/MAC address pair exists in the ARP cache, the system determines the correct BIG-IP system interface to use, and then forwards the packets to that MAC address. If no entry for the IP address/MAC address pair exists in its ARP cache, the system broadcasts an ARP request to hosts on the network and then behaves in the following way:

- If a host sends an ARP response (its MAC address) within two seconds of the ARP request, the BIG-IP system stores that MAC address pair in its ARP cache for subsequent use, and sets the state of the entry to **RESOLVED**. The system then determines the correct interface and sends the data packets to that MAC address. For more information on the **RESOLVED** state, see *Understanding ARP entry states* on this page.
- If no host sends an ARP response after two seconds have passed, the BIG-IP system repeatedly broadcasts the ARP request until a host sends a response, or until the maximum number of allowed requests is reached. (The maximum number of requests to the same host that the BIG-IP system can make is a setting that you configure.) If the system sends the maximum number of ARP requests and does not receive a response, the host is declared to be unreachable, and the system sets the state of the entry to **DOWN**. For more information on the **DOWN** state, see *Understanding ARP entry states* on this page.
- If the BIG-IP system receives a second packet targeted for the same destination within two seconds of making an ARP request, the system discards the original packet and replaces it with the second packet, and then sends another ARP request.

  If the BIG-IP system needs to send more packets to that same host later, and the ARP cache entry pertaining to that host has not timed out yet, the BIG-IP system can send the packets to the host without sending another ARP request first.

Understanding ARP entry states

Each entry in the ARP cache has a state associated with it. When you use the Configuration utility to view the entries in the ARP cache, you can view the state of each entry. The possible states for an entry are **RESOLVED**, **INCOMPLETE**, and **DOWN**.

The BIG-IP system marks an ARP cache entry as ***RESOLVED*** when the system has successfully received an ARP response (a MAC address) for the requested IP address within two seconds of initiating the request. An entry in a **RESOLVED** state remains in the ARP cache until the timeout period has expired.

The BIG-IP system marks an ARP cache entry as ***INCOMPLETE*** when the system has made one or more ARP requests within the maximum number of requests allowed, but has not yet received a response.

The BIG-IP system marks an ARP cache entry as ***DOWN*** when the system has made the maximum number of requests allowed, and still receives no response. In this case, the system discards the packet, and sends an **ICMP host unreachable** message to the sender. An entry with a **DOWN** state remains in the ARP cache until the first of these events occurs:

- Twenty seconds elapse.
- The BIG-IP system receives either a resolution response or a gratuitous ARP from the destination host. (A ***gratuitous ARP*** is an ARP message that a host sends without having been prompted by an ARP request.)
- You explicitly delete the entry from the ARP cache.

Responding to ARP requests

By default, the BIG-IP system does not respond to a certain types of ARP requests. More specifically, the system does not respond to ARP requests sent from any firewall that uses a multicast IP address as its source address.

You can change this behavior to allow the BIG-IP system to respond to this type of ARP request, by configuring the bigdb™ key **TM.AllowEthernetSourceType** as follows:

```
bigpipe db TM.AllowEthernetSourceType unicast-multicast
```

Configuring static entries in the ARP cache

Static entries in the ARP cache do not have a timeout value, and therefore remain in the ARP cache until you explicitly delete them. By adding static entries to the ARP cache, you reduce the number of ARP requests that the BIG-IP system must make to determine destination MAC addresses.

Using the Configuration utility, you can add entries to the ARP cache of the BIG-IP system. You can also view, modify, and delete any existing static entries.

Adding static entries

Adding a static entry for a destination server to the ARP cache saves the BIG-IP system from having to send an ARP broadcast request for that destination server. This can be useful, for example, for specifying a multicast or other special MAC address for servers or gateways.

You can explicitly add entries to the ARP cache on the BIG-IP system. Because static entries do not have a timeout value, they remain in the ARP cache until you explicitly delete them. When you add static entries to the ARP cache, the BIG-IP system can determine the MAC address for an IP address without having to broadcast an ARP request. This can be useful when you want the system to forward packets to a special MAC address, such as a shared MAC address, or you want to ensure that the MAC address never changes for a given IP address.

Adding static entries to the ARP cache is simple. You merely specify an IP address and its corresponding MAC address. Then, when the BIG-IP system must forward packets to that IP address, the system checks the ARP cache to find the MAC address. The system can then check the VLAN's layer 2 forwarding table to determine the appropriate outgoing interface. (For more information on the layer 2 forwarding table, see Chapter 5, *Configuring VLANs and VLAN Groups*).

To add a static entry to the ARP cache

1. On the Main tab of the navigation pane, expand **Network** and click **ARP**.
   This displays a list of any existing static entries in the ARP cache.

2. In the upper-right corner, click **Create**.
   The ARP screen opens.

3. In the **IP Address** box, type the IP address for a destination host.

4. In the **MAC Address** box, type the MAC address for the destination host specified in the **IP Address** box.

5. Click **Finished**.

Viewing static entries

Using the Configuration utility, you can view a list of the static entries that you have added to the ARP cache. When you display the list of static entries in the ARP cache, each entry includes an IP address and its corresponding MAC address.

To view static entries

On the Main tab of the navigation pane, expand **Network**, and click **ARP**.

By default, this displays a list of existing static entries in the ARP cache. If you have not yet added any static entries to the ARP cache, the list displays the message **No records to display**.

Modifying static entries

Sometimes, the MAC address of a destination host changes, while the IP address stays the same. This requires you to modify any static entry that you might have previously added to the ARP cache for that host. When you modify a static ARP cache entry, you change the MAC address associated with the IP address.

To modify a static entry

1. On the Main tab of the navigation pane, expand **Network** and click **ARP**.
   This displays a list of existing static entries in the ARP cache.

   Note: *If no entries exist, the screen displays the message* ***No records to display***.
2. In the IP address column, click an IP address.
   This displays the MAC address that you associated with this IP address when you added the static entry.
3. In the **MAC Address** box, delete the current MAC address and type a new MAC address.
4. Click **Update**.

Deleting static entries

At any time, you can remove a static entry from the ARP cache. A common reason for deleting an ARP cache entry is when you remove the corresponding destination host from the network. In this case, the BIG-IP system no longer needs to store MAC address information for that host.

To delete a static entry

1. On the Main tab of the navigation pane, expand **Network** and click **ARP**.
   This displays a list of existing static entries in the ARP cache.
2. In the IP Address column, locate the entry you want to delete.
3. Check the Select box to the left of the IP address.
4. Click **Delete**.
   A confirmation message appears.
5. Click **Delete** again.
   This removes the entry from the ARP cache.

Configuring dynamic entries in the ARP cache

If you do not want to add a static entry into the ARP cache for every destination host on the network, you can use ARP to add these entries dynamically. The primary functions of ARP are to automatically broadcast requests for MAC addresses, and to dynamically store those responses in the ARP cache.

Configuring dynamic entries is slightly different from configuring static entries:

- You specify a set of values that applies globally to all dynamic entries. Configuring these global options affects the way that ARP treats dynamic entries in the ARP cache. For more information, see *Configuring global options* on this page.
- You do not explicitly add dynamic entries to the ARP cache, because ARP adds those entries for you. Also, you do not modify dynamic entries. You can, however, view and delete dynamic entries from the ARP cache. For more information, see *Viewing dynamic entries*, on page 9-9 and *Deleting dynamic entries*, on page 9-10.

Configuring global options

You can configure a number of options that affect the way that ARP behaves. While all of these options have default values, you can change these values to suit your needs. Table 9.1 lists and describes these options. Following the table are more detailed descriptions of each option.

Option	Description	Default Value
Dynamic Timeout	Specifies the maximum number of seconds that a dynamic entry can remain in the ARP cache before the BIG-IP system automatically removes it.	**300**
Maximum Dynamic Entries	Specifies the maximum number of dynamic entries that the ARP cache can hold at any given time.	**2048**
Request Retries	Specifies the number of times that the BIG-IP system sends ARP requests for an unresolved address, before determining that the remote address is in a **down** state or not on the network.	**6**
Reciprocal Update	Specifies whether the BIG-IP system should add an entry to the ARP cache as a result of receiving an ARP broadcast request from another host on the network.	Enabled (checked)

Table 9.1 *Global configuration options for ARP*

Specifying a dynamic timeout value

With the **Dynamic Timeout** option, you can specify the maximum number of seconds that a dynamic entry can remain in the ARP cache before the BIG-IP system automatically removes it. The default value is **300**.

Once you have configured this value and the system dynamically adds an entry to the ARP cache, the seconds begin to count down toward **0** for that entry. When the value reaches **0**, the BIG-IP system automatically deletes the entry from the cache. If the entry is actively being used as the time approaches **0**, ARP attempts to refresh the entry by sending an ARP request.

At any given time, you can view the seconds that remain for a dynamic entry. You do this by viewing the entry in the ARP cache. For more information, see *Viewing dynamic entries*, on page 9-9.

Specifying a dynamic entry limit

You can configure the **Maximum Dynamic Entries** option to limit the number of dynamic entries that the BIG-IP system can hold in the ARP cache at any given time. The default value is **2048**.

This setting relates to dynamic entries only and has no effect on the number of static entries that the ARP cache can hold. Therefore, if the number of dynamic entries in the cache reaches the limit that you specified, you can still add static entries to the cache. This is possible because the system can remove an older dynamic entry prematurely to make space for a new static entry that you add.

◆ **Note**

*The value of the **Maximum Dynamic Entries** option should be large enough to maintain entries for all directly-connected hosts with which the BIG-IP system must communicate. If you have more than 2000 hosts that are directly connected to the BIG-IP system, you should specify a value that exceeds the default value of **2048**.*

Specifying an ARP request limit

When the BIG-IP system needs a MAC address for a given IP address and does not have the information in its ARP cache, the system must broadcast an ARP request to the hosts on the network (or VLAN). Sometimes, the BIG-IP system receives no response to this request and so resends the request. The **Request Retries** option specifies the number of times that the BIG-IP system can resend an ARP request before finally marking the host as unreachable. The default value is **6**.

Specifying reciprocal update

The information stored in the ARP cache is typically the IP addresses and MAC addresses that the BIG-IP system receives in response to its own ARP requests. However, when you enable the **Reciprocal Update** option, the BIG-IP system can also store information that it learns as a result of other hosts on the network sending ARP broadcast requests (that is, who-has packets) to the BIG-IP system. By default, the **Reciprocal Update** option is enabled.

Depending on how you set this option, ARP behaves in these ways:

- **Enabled**
  When you enable the **Reciprocal Update** option, the BIG-IP system creates an entry in the ARP cache whenever the system receives who-has packets from another host on the network. Enabling this option slightly enhances performance by eliminating the need for the BIG-IP system to perform an additional ARP exchange later.

- **Disabled**
  When you disable the **Reciprocal Update** option, the BIG-IP system does not add an entry to the ARP cache in response to receiving who-has packets from a host. Instead, the system creates an ARP cache entry for a host only when the system needs to send non-ARP traffic to that host. If the BIG-IP system never needs to send non-ARP traffic to the host, then the system never dynamically adds an entry for that host.

  Disabling this option provides a security benefit, by preventing a malicious action known as ARP poisoning. ***ARP poisoning*** occurs when a host is intentionally altered to send an ARP response containing a false MAC address. By disabling the **Reciprocal Update** option, the BIG-IP system cannot add that false information to its ARP cache.

Viewing dynamic entries

Using the Configuration utility, you can view a list of the dynamic entries that ARP has added to the ARP cache. When you display the list of dynamic entries in the ARP cache, each entry shows this information:

- IP address of the destination host
- MAC address of the destination host
- The VLAN of the destination host
- The number of seconds remaining before the entry times out
- The state of the entry. Valid states are: **RESOLVED, INCOMPLETE,** and **DOWN**. For detailed information on these states, see *Understanding ARP entry states*, on page 9-2.

To view dynamic entries

1. On the Main tab of the navigation pane, expand **Network**, and click **ARP**.
2. On the menu bar, click **Dynamic List**.
   This displays a list of dynamic entries in the ARP cache. If no dynamic entries exist, the screen displays the message **No records to display**.

Deleting dynamic entries

At any time, you can remove a dynamic entry from the ARP cache. A common reason for deleting an ARP cache entry is when you move a host from one VLAN to another, or you change the MAC address associated with that host. By removing a dynamic entry, you ensure that ARP learns the new information before the timeout value for the entry expires.

To delete a dynamic entry

1. On the Main tab of the navigation pane, expand **Network** and click **ARP**.
   This displays a list of existing static entries in the ARP cache.
2. On the menu bar, click **Dynamic List**.
   This displays a list of dynamic entries in the ARP cache.

   Note: *If no entries exist, the screen displays the message* ***No records to display****.*
3. In the IP Address column, locate the entry you want to delete.
4. Check the Select box to the left of the IP address.
5. Click **Delete**.
   A confirmation message appears.
6. Click **Delete** again.
   This removes the entry from the ARP cache.

10

Working with Trunks

- Introducing trunks
- Creating a trunk
- Managing trunks

Introducing trunks

A ***trunk*** is a logical grouping of interfaces on the BIG-IP system. When you create a trunk, this logical group of interfaces functions as a single interface. The BIG-IP system uses a trunk to distribute traffic across multiple links, in a process known as ***link aggregation***. With link aggregation, a trunk increases the bandwidth of a link by adding the bandwidth of multiple links together. For example, four fast Ethernet (100 Mbps) links, if aggregated, create a single 400 Mbps link.

With one trunk, you can aggregate a maximum of eight links. For optimal performance, you should aggregate links in powers of two. Thus, you ideally aggregate two, four, or eight links.

The purpose of a trunk is two-fold: To increase bandwidth without upgrading hardware, and to provide link failover if a member link becomes unavailable.

You can use trunks to transmit traffic from a BIG-IP system to another vendor switch. Two systems that use trunks to exchange frames are known as ***peer systems***.

How do trunks work?

In a typical configuration where trunks are configured, the member links of the trunk are connected through Ethernet cables to corresponding links on a peer system. Figure 10.1 shows an example of a typical trunk configuration with two peers and three member links on each peer.

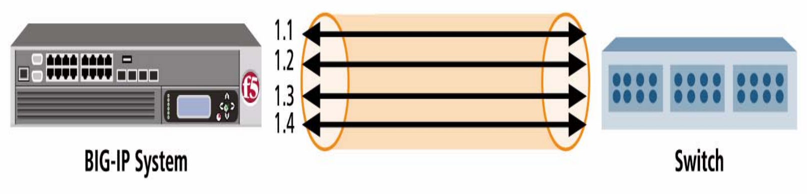


Figure 10.1 *Example of a trunk configured for two switches*

A primary goal of the trunks feature is to ensure that frames exchanged between peer systems are never sent out of order or duplicated on the receiving end. The BIG-IP system is able to maintain frame order by using the source and destination addresses in each frame to calculate a hash value, and then transmitting all frames with that hash value on the same member link.

The BIG-IP system automatically assigns a unique MAC address to a trunk. This MAC address becomes the source address for frames that the system transmits, and the destination address for frames that the system receives.

However, the BIG-IP system still uses the MAC address of an individual member link as the source address for any LACP control frames. For more information on LACP, see *Overview of LACP*, following.

The BIG-IP system uses the lowest-numbered interface in a trunk as a ***reference link***. The BIG-IP system uses the reference link to take certain aggregation actions, such as implementing the automatic link selection policy. For frames coming into the reference link, the BIG-IP system load balances the frames across all member links that the BIG-IP system knows to be available. For frames going from any link in the trunk to a destination host, the BIG-IP system treats those frames as if they came from the reference link.

Overview of LACP

A key aspect of trunks is Link Aggregation Control Protocol, or LACP. Defined by IEEE standard 802.3ad, ***LACP*** is a protocol that detects error conditions on member links and redistributes traffic to other member links, thus preventing any loss of traffic on the failed link. On a BIG-IP system, LACP is an optional feature that you can configure.

You can also customize LACP behavior. For example, you can specify the way that LACP communicates its control messages from the BIG-IP system to a peer system. You can also specify the rate at which the BIG-IP system exchanges LACP packets with a peer system. If you want to affect the way that the BIG-IP system chooses links for link aggregation, you can specify a link control policy. For more information, see *Creating a trunk*, on page 10-3.

Creating a trunk

You create a trunk using the Configuration utility. The BIG-IP system offers several settings that you can configure for a trunk. These settings are summarized in Table 10.1.

Setting	Description	Default Value
Name	Specifies a unique name for the trunk. For more information, see *Specifying a trunk name*, on page 10-4.	No default value
Interfaces	Specifies the interfaces that constitute member links of the trunk. For more information, see *Specifying interfaces for a trunk*, on page 10-4.	No default value
LACP	Enables or disables the Link Aggregation Control Protocol (LACP). For more information, see *Enabling LACP*, on page 10-5.	Unchecked
Link Mode	Specifies the way that member links communicate over LACP. Possible values are **Active** and **Passive**. For more information, see *Specifying the LACP mode*, on page 10-5.	**Active**
Link Timeout	Specifies the length of time that the BIG-IP system sends control packets. Possible values are **Short** and **Long**. For more information, see *Specifying the LACP timeout*, on page 10-6.	**Long**
Link Selection Policy	Specifies the policy that the BIG-IP uses to select a link for processing traffic. Possible values are **Auto** and **Maximum Bandwidth**. For more information, see *Specifying a link selection policy*, on page 10-6.	**Auto**

Table 10.1 *Configuration settings for a trunk*

Use the following procedure to create a trunk. For detailed information about each setting, see the sections following the procedure.

To create a trunk

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens.
2. In the upper-right corner of the screen, click the **Create** button.
   Another Trunks screen opens.
3. In the **Name** box, type a unique name for the trunk.
4. For the **Interfaces** setting, in the **Available** box, select an interface that you want to include in the trunk, and using the Move button (**<<**), move the interface to the **Members** box.
5. Repeat the previous step as necessary.

6. If you want to enable the LACP feature, check the **LACP** box, and do the following:

   a) From the **LACP Mode** list, select **Passive** mode, or retain the default mode (**Active**).

   b) From the **LACP Timeout** list, select **Short**, or retain the default timeout value (**Long**).

7. From the **Link Selection Policy** list, select or retain a link selection policy.

8. Click **Finished**.

Specifying a trunk name

You can use the **Name** setting to specify a unique name for the trunk. This setting is required.

Specifying interfaces for a trunk

Using the **Interfaces** setting, you specify the interfaces that you want the BIG-IP system to use as member links for the trunk. Once you have created the trunk, the BIG-IP system uses these interfaces to perform link aggregation.

As stated earlier, the BIG-IP system uses the lowest-numbered interface as the reference link. The system uses the reference link to negotiate links for aggregation. For more information on link negotiation, see *Specifying a link selection policy*, on page 10-6.

The interfaces that you specify for the trunk must operate at the same media speed, and must be set at full-duplex mode. Otherwise, the BIG-IP system cannot aggregate the links. Because these media properties are dynamic rather than static (due to auto-negotiation), the **lacpd** service routinely monitors the current status of these properties and negotiates the links for aggregation accordingly. Thus, when the status of these properties qualifies a link to become a working member link, the system adds the link to the aggregation, and the link can begin accepting traffic. For information on setting media properties for an interface, see ***Platform Guide: 1500, 3400, 6400, and 6800***.

Any interface that you assign to a trunk must be an untagged interface. Furthermore, you can assign an interface to one trunk only; that is, you cannot assign the same interface to multiple trunks. Because of these restrictions, the only interfaces that appear in the **Interfaces** list in the Configuration utility are untagged interfaces that are not assigned to another trunk. Therefore, before creating a trunk and assigning any interfaces to it, you should verify that each interface for the trunk is an untagged interface.

After creating the trunk, you assign the trunk to one or more VLANs, using the same VLAN screen that you normally use to assign an individual interface to a VLAN. For information on assigning a trunk to a VLAN, see Chapter 5, *Configuring VLANs and VLAN Groups*.

If you are using one of the spanning tree protocols (STP, RSTP, or MSTP), the BIG-IP system sends and receives spanning tree protocol packets on a trunk, rather than on individual member links. Likewise, use of a spanning tree protocol to enable or disable learning or forwarding on a trunk operates on all member links together, as a single unit.

Enabling LACP

As an option, you can enable LACP on a trunk. Containing a service called **lacpd**, LACP is an IEEE-defined protocol that exchanges control packets over member links. The purpose of LACP is to detect link error conditions such as faulty MAC devices and link loopbacks. If LCAP detects an error on a member link, the BIG-IP system removes the member link from the link aggregation and redistributes the traffic for that link to the remaining links of the trunk. In this way, no traffic destined for the removed link is lost. LACP then continues to monitor the member links to ensure that aggregation of those links remains valid.

By default, the LACP feature is disabled, to ensure backward compatibility with previous versions of the BIG-IP system. If you create a trunk and do not enable the LACP feature, the BIG-IP system does not detect link error conditions, and therefore cannot remove the member link from link aggregation. The result is that the system cannot redistribute the traffic destined for that link to the remaining links in the trunk, thereby causing traffic on the failed member link to be lost.

◆ **Important**

To use LACP successfully, you must enable LACP on both peer systems.

Specifying the LACP mode

The **LACP Mode** setting appears on the Trunks screen only when you check the **LACP** setting. You use the **LACP mode** setting to specify the method that LACP uses to send control packets to the peer system. The two possible modes are:

- **Active mode**
  You specify **Active** mode if you want the system to periodically send control packets, regardless of whether the peer system has issued a request. This is the default setting.

- **Passive mode**
  You specify **Passive** mode if you want the system to send control packets only when the peer system issues a request, that is, when the LACP mode of the peer system is set to **Active**.

If you set only one of the peer systems to **Active** mode, the BIG-IP system uses **Active** mode for both systems. Also, whenever you change the LACP mode on a trunk, LACP renegotiates the links that it uses for aggregation on that trunk.

◆ **Tip**

*We recommend that you set the LACP mode to **Passive** on one peer system only. If you set both systems to **Passive** mode, no control packets are sent.*

Specifying the LACP timeout

The **LACP Timeout** setting appears on the Trunks screen only when you check the **LACP** setting. You use the **LACP Timeout** setting to specify the number of seconds that the system waits before sending control packets to the peer system. The timeout value only applies when the LACP mode is set to **Active** on at least one of the systems. If both systems are set to **Passive** mode, LACP does not send control packets.

If LACP sends three consecutive control packets without receiving a response from the peer system, LACP removes that member link from link aggregation.

The two possible timeout values are:

- **Short**
  When you set the timeout value to **Short**, the BIG-IP system sends LACP control packets to the peer system once every second. If this value is set to **Short** and LACP receives no peer response after sending three consecutive packets, LACP removes the link from aggregation in three seconds.

- **Long**
  When you set the timeout value to **Long**, the BIG-IP system sends LACP control packets to the peer system once every 30 seconds. A timeout value of **Long** is the default setting. If set to **Long** and LACP receives no peer response after sending three consecutive packets, LACP removes the link from aggregation in ninety seconds.

Whenever you change the LACP timeout value on a trunk, LACP renegotiates the links that it uses for aggregation on that trunk.

Specifying a link selection policy

In order for the BIG-IP system to aggregate links, the media speed and duplex mode of each link must be the same on both peer systems. Because media properties can change dynamically, the BIG-IP system monitors these properties regularly, and if it finds that the media properties of a link are mismatched on the peer systems, the BIG-IP system must determine which links are eligible for aggregation.

The way the system determines eligible links depends on a link selection policy that you choose for the trunk. When you create a trunk, you can choose one of two possible policy settings: **Auto** and **Maximum Bandwidth**.

◆ **Note**

The link selection policy feature represents an F5 Networks enhancement to the standard IEEE 802.3ad specification for LACP.

Understanding automatic link selection

When you set the link selection policy to **Auto** (the default setting), the BIG-IP system uses the lowest-numbered interface of the trunk as a reference link. (A ***reference link*** is a link that the BIG-IP uses to make a link aggregation decision.) The system then aggregates any links that have the same media properties and are connected to the same peer as the reference link.

For example, using Figure 10.1, on page 10-1, suppose that you created a trunk to include interfaces 1.2 and 1.3, each with a media speeds of 100 Mbps, and interface 1.4, with a different media speed of 1 Gbps. If you set the link selection policy to **Auto**, the BIG-IP system uses the lowest-numbered interface, 1.2, as a reference link. The reference link operates at a media speed of 100 Mbps, which means that the system aggregates all links with that media speed (interfaces 1.2 and 1.3). The media speed of interface 1.4 is different (1 Gbps), and therefore is not considered for link aggregation. Only interfaces 1.2 and 1.3 become working member links and start carrying traffic.

If the media speed of interface 1.4 changes to 100 Mbps, the system adds that interface to the aggregation. Conversely, if the media speed of interface 1.4 remains at 1 Gbps, and the speed of the reference link changes to 1 Gbps, then interfaces 1.2 and 1.4 become working members, and 1.3 is now excluded from the aggregation and no longer carries traffic.

Understanding maximum bandwidth link selection

When you set the link selection policy to **Maximum Bandwidth**, the BIG-IP system aggregates the subset of member links that provide the maximum amount of bandwidth to the trunk.

Continuing with our previous example, if interfaces 1.2 and 1.3 each operate at a media speed of 100 Mbps, and interface 1.4 operates at speed of 1 Gbps, then the system selects only interface 1.4 as a working member link, providing 1 Gbps of bandwidth to the trunk. If the speed of interface 1.4

drops to 10 Mbps, the system then aggregates links 1.2 and 1.3, to provide a total bandwidth to the trunk of 200 Mbps. The peer system detects any non-working member links and configures its aggregation accordingly.

◆ **Tip**

To ensure that link aggregation operates properly, make sure that both peer systems agree on the link membership of their trunks.

Managing trunks

After you have created your trunks, you can manage them in several ways. You can:

- View a list of existing trunks
- View or modify trunk properties
- Add a trunk to a VLAN
- Delete a trunk
- Manage interfaces for a trunk

As with trunk creation, you manage trunks using the Configuration utility.

Viewing a list of trunks

Before you create a new trunk, you might want to view a list of existing trunks. When you use the Configuration utility to view a list of trunks, you not only see the trunk names, but also some data about each trunk:

- Trunk status (**UP** or **DOWN**)
- MAC address of the trunk
- LACP mode (**Active** or **Passive**)
- Number of interfaces (member links) in the trunk
- Current trunk capacity

To view a list of trunk names and data

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens.
2. View the list of trunk names and associated data.

Viewing or modifying trunk properties

For any existing trunk, you can use the Configuration utility to view or modify the properties of that trunk. These properties consist of not only the settings that you configured for the trunk, but also other read-only LACP-specific properties that conform to the IEEE 802.3ad standard.

The read-only LACP properties you can view for an existing trunk are as follows. Note that the term ***actor*** refers to the local endpoint of the trunk, and ***peer*** refers to the remote endpoint of the trunk.

- MAC address of the trunk
- Actor ID, Actor Key, and Actor Priority
- Peer ID, Peer Key, and Peer Priority

For detailed information these LACP parameters, see the IEEE 802.3ad specification.

The modifiable properties that you can view for a trunk are:

- Interfaces that are member links of the trunk
- LACP settings (such as mode and timeout)
- Link selection policy

To view or modify properties of a trunk

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens, showing the list of existing trunks.
2. Click a trunk name.
   The properties screen for that trunk opens.
3. In the Properties area of the screen, view the properties.
4. In the Configuration area of the screen, view or modify the setting values.
   For information on selecting values for these settings, see *Creating a trunk*, on page 10-3.
5. If you modified any values, click **Update**. Otherwise, click **Cancel**.

Adding a trunk to a VLAN

After creating a trunk, you can add the trunk to a VLAN. You add a trunk to a VLAN by using the VLAN screens of the Configuration utility. For more information, see Chapter 5, *Configuring VLANs and VLAN Groups*.

Deleting a trunk

You can use the Configuration utility to delete an existing trunk. When you delete a trunk, individual interfaces are no longer considered to be member links of a trunk and are no longer aggregated.

Remember that when you added the interfaces to the trunk, the BIG-IP system first required you to remove the individual interfaces from VLAN membership. Therefore, after deleting the trunk, if you want the individual interfaces of the trunk to become VLAN members again, you must explicitly assign them to one or more VLANs, using the VLANs screens of the Configuration utility.

You cannot delete any trunk that is a member of VLAN or that participates in Spanning Tree Protocol. For this reason, you must remove the trunk from any VLAN to which it is assigned, and from STP configuration, before you delete the trunk.

To delete a trunk

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens, showing the list of existing trunks.
2. In the Name column, locate the name of the trunk you want to delete.
3. To the left of the trunk name, check the Select box.
4. Click the **Delete** button.
   A confirmation message appears.
5. Click **Delete** to delete the trunk.

Managing interfaces for a trunk

You can manage the interfaces of a trunk by adding them to or deleting them from a trunk. You can also view trunk-related properties of an interface in the trunk.

◆ **Note**

The following procedure for adding an interface to a trunk is equivalent to modifying the ***Interfaces*** *property of the trunk, as described in step 4 of the section* ***To view or modify properties of a trunk****, on page 10-10.*

To add an interface to a trunk by viewing trunk resources

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens, showing the list of existing trunks.
2. Click a trunk name.
   The properties screen for that trunk opens.
3. On the menu bar, click **Resources**.
   This displays the list of interfaces assigned to the trunk, along with some interface properties.
4. In the upper right corner of the screen, click **Add**.
5. For the **Interfaces** setting, in the **Available** box, select an interface that you want to include in the trunk, and using the Move button (**<<**), move the interface to the **Members** box.
6. Repeat the previous step as necessary.
7. Click **Update**.

To remove an interface from a trunk

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens, showing the list of existing trunks.
2. Click a trunk name.
   The properties screen for that trunk opens.

3. On the menu bar, click **Resources**.
   This displays the list of interfaces assigned to the trunk, along with some interface properties.
4. In the Name column, locate the interface that you want to remove, and check the Select box to the left of the Status column.
5. Click **Delete**.
   A confirmation message appears.
6. Click **Delete** to remove the interface from the trunk.

To view trunk-related properties of an interface

1. On the Main tab, expand **Network**, and click **Trunks**.
   The Trunks screen opens, showing the list of existing trunks.
2. Click a trunk name.
   The properties screen for that trunk opens.
3. On the menu bar, click **Resources**.
   This displays the list of interfaces assigned to the trunk, along with some interface properties.
4. In the Name column, click the interface for which you want to view trunk-related properties.
   This displays trunk-related properties for the interface.

◆ **Tip**

*To view the set of properties for an interface, see Chapter 7, **Working with Interfaces**.*

11

Configuring Packet Filters

- Introducing packet filtering
- Configuring global settings
- Creating packet filter rules
- Managing packet filter rules

Introducing packet filtering

Packet filters enhance network security by specifying whether a BIG-IP system interface should accept or reject certain packets based on criteria that you specify. Packet filters enforce an access policy on incoming traffic. They apply to incoming traffic only.

You implement packet filtering by creating packet filter rules, using the Configuration utility. The primary purpose of a ***packet filter rule*** is to define the criteria that you want the BIG-IP system to use when filtering packets. Examples of criteria that you can specify in a packet filter rule are:

- The source IP address of a packet
- The destination IP address of a packet
- The destination port of a packet

You specify the criteria for applying packet filter rules within an expression. When creating a packet filter rule, you can instruct the Configuration utility to build an expression for you, in which case you need only choose the criteria from predefined lists, or you can write your own expression text, using the syntax of the **tcpdump** utility. For more information on the **tcpdump** utility, see the online man page for the **tcpdump** command.

◆ **Note**

Packet filter rules are unrelated to iRules™.

You can also configure global packet filtering that applies to all packet filter rules that you create. The following sections describe how to set global packet filtering options, and how to create and manage individual packet filters rules.

Configuring global settings

Global settings for packet filtering are divided into two categories: Properties and Exemptions. The BIG-IP system applies global settings to all packets coming into the BIG-IP system. You can configure these settings using the Configuration utility.

◆ **Important**

Note that one of the global settings, ***Packet Filtering****, enables packet filtering. When you disable this setting, no packet filter settings or packet filter rules operate, and the BIG-IP system allows all traffic by default.*

To configure global settings

1. On the Main tab of the navigation pane, expand **Network**, and click **Packet Filters**.
   The Packet Filters screen opens.
2. From the **Packet Filtering** list, select **Enabled**.
   This displays additional settings.

   Note: *See* ***Important*** *note preceding this procedure.*
3. Configure the values for all properties and exemptions.
   For detailed information on the global properties and exemptions, see *Configuring global properties*, following, and *Configuring exemptions*, on page 11-3.

   Note: *Before configuring the* ***Unhandled Packet Action*** *setting, see the warning information in* ***Controlling unhandled packets****, on page 11-3.*
4. Click **Update**.

Configuring global properties

You can configure three specific global properties for packet filtering. Table 11.1 lists and describes the properties you can set for global packet filtering. Following the table are more detailed descriptions of these properties.

Property	Description	Default Value
Packet Filtering	Indicates whether the packet filtering feature is enabled or disabled.	**Disabled**
Unhandled Packet Action	Determines how the BIG-IP system handles packets that do not match any packet filter rule.	**Accept**
Options	Provides two options that you can set on packet filtering. You can filter established connections, and, when the packet filter rule rejects a packet, you can instruct the BIG-IP system to send an ICMP **administratively prohibited** error instead of a **connection refused** error.	Disabled (unchecked)

Table 11.1 *Global packet filtering properties*

Enabling packet filtering

Before you can implement packet filtering on the BIG-IP system, you must enable the packet filter feature. You do this by changing the **Packet Filtering** setting to **Enabled**. The default setting for packet filtering is **Disabled**.

Controlling unhandled packets

Sometimes a packet does not match any of the criteria that you have specified in the packet filter rules that you have created. For this reason, you must configure the **Unhandled Packet Action** property, which specifies the action that the BIG-IP system should take when the packet does not match packet filter rule criteria.

Possible values for this setting are **Accept**, **Discard,** and **Reject.** The default value is **Accept**.

◆ **WARNING**

*Changing the default value of the **Unhandled Packet Action** property can produce unwanted consequences. Before changing this value to **Discard** or **Reject**, make sure that any traffic that you want the BIG-IP system to accept meets the criteria specified in your packet filter rules.*

Specifying other options

Using the **Options** property, you can configure two other options:

- **Filter established connections**
  When you enable (check) this option, the BIG-IP system filters all ingress packets, even if the packets are part of an existing connection. The default setting is disabled (unchecked). Note that checking this option does not typically enhance security, and can impact system performance.

- **Send ICMP error on packet reject**
  When you enable (check) this option, the system sends, an ICMP type 3 (destination unreachable), code 13 (administratively prohibited) packet when an ingress packet is rejected. When you disable (uncheck) this option, the BIG-IP system sends an ICMP reject packet that is protocol-dependent. The default setting for this option is disabled (unchecked).

Configuring exemptions

There are a number of exemptions you can set for packet filtering. When filtering packets, the BIG-IP system always applies these exemptions, effectively overriding certain criteria you might have previously set within an individual packet filter rule.

Table 11.2 lists and describes the exemptions you can set for packet filtering. Following the table are descriptions of each setting and information on how to configure them. For the basic procedure on configuring these exemptions, see *To configure global settings*, on page 11-2.

Exemption	Description	Default Value
Protocols	Specifies whether the packet filter should always accept ARP or important ICMP traffic.	No default value
MAC Addresses	Specifies which MAC addresses to always allow. Selecting **Always Accept** allows you to specify one or more Mac addresses.	**None**
IP Addresses	Specifies IP addresses to always allow. Selecting **Always Accept** allows you to specify one or more IP addresses.	**None**
VLANs	Specifies which ingress VLANs to always allow. Selecting **Always Accept** allows you to specify one or more VLANs.	**None**

Table 11.2 *Global packet filtering exemptions*

Specifying protocols as exemptions

With the **Protocols** setting, you can specify whether ARP and certain ICMP messages are exempt from packet filtering. The individual settings are:

- **Always accept ARP**
  When you enable (check) this setting, the system automatically accepts all ARP packets and therefore does not subject them to packet filtering. The default setting is enabled (checked).

- **Always accept important ICMP**
  When you enable (check) this setting, the system automatically accepts the following ICMP packet types for IPv4, and therefore does not subject them to packet filtering:

  - **UNREACH**
  - **SOURCEQUENCH**
  - **REDIRECT**
  - **TIMEXCEED**

  In addition, the system accepts the following ICMP packet types for IPv6:

  - **DST_UNREACH**
  - **PACKET_TOO_BIG**
  - **TIME_EXCEEDED**
  - **PARAM_PROB**
  - **LISTENER_QUERY**
  - **LISTENER_REPORT**

- **LISTENER_DONE**
- **ROUTER_SOLICIT**
- **ROUTER_ADVERT**
- **NEIGHBOR_SOLICIT**
- **NEIGHBOR_ADVERT**
- **REDIRECT**

The default setting is enabled (checked).

Specifying MAC addresses as exemptions

You can use the **MAC Addresses** setting to exempt traffic from certain MAC addresses from packet filtering. Possible values are:

- **Always Accept**
  When you select this value, a **MAC Address List** setting appears. You can then specify one or more MAC addresses from which traffic should be exempt from packet filtering.
- **None**
  When you select this value, traffic from all MAC addresses is subject to packet filtering, according to existing packet filter rule criteria. This is the default value.

To specify one or more MAC addresses, locate the **MAC addresses** setting and select **Always Accept**. Then, in the **MAC Address List** area, type a MAC address and click **Add**. Repeat this process for each MAC address that you want the BIG-IP system to exempt from packet filtering.

Specifying IP addresses as exemptions

You can use the **IP Addresses** setting to exempt traffic from certain IP addresses from packet filtering. Possible values are:

- **Always Accept**
  When you select this value, an **IP Address List** setting appears. You can then specify one or more IP addresses from which traffic should be exempt from packet filtering.
- **None**
  When you select this value, traffic from all IP addresses is subject to packet filtering, according to existing packet filter rule criteria. This is the default value.

To specify one or more IP addresses, locate the **IP Addresses** setting and select **Always Accept**. Then, in the **IP Address List** area, type an IP address and click **Add**. Repeat this process for each IP address that you want the BIG-IP system to exempt from packet filtering.

Specifying VLANs as exemptions

Using the **VLANs** setting, you can configure the BIG-IP system so that traffic from one or more specified VLANs is exempt from packet filtering. In this case, the system does not attempt to match packets from the specified VLAN or VLANs to any packet filter rule. Instead, the BIG-IP system always accepts traffic from the specified VLAN or VLANs.

For example, if you specify VLAN **internal**, then no incoming packets from VLAN **internal** are subject to packet filtering, even if a packet matches the criteria of a packet filter rule.

Possible values are:

- **Always Accept**
  When you select this value, a **VLAN List** setting appears. You can then specify one or more VLANs from which traffic should be exempt from packet filtering.
- **None**
  When you select this value, traffic from all VLANs is subject to packet filtering, according to existing packet filter rule criteria. This is the default value.

To specify one or more VLANs, locate the **VLANs** setting and select **Always Accept**. Then, in the **VLAN List** area, select a VLAN name in the **Available** box and using the **Move** button (**<<**), move the VLAN name to the **Selected** box. Repeat this process for each VLAN that you want the BIG-IP system to exempt from packet filtering.

Creating packet filter rules

Packet filter rules are criteria statements that the BIG-IP system uses for filtering packets. The BIG-IP system attempts to match packet filter rules with an incoming packet, and if a match exists, determines whether or not to accept or reject the packet.

When you create a packet filter rule, you configure several settings, and then you define the criteria that you want the BIG-IP system to use to filter the traffic. To create the rule, you configure the Configuration and the Filter Expression areas of the New Packet Filter Rule screen.

To create a packet filter rule

1. On the Main tab of the navigation pane, expand **Network**, and click **Packet Filters**.
   The Packet Filters screen opens.

   Note: *If you have not enabled the Packet Filter feature, you can still create a packet filter rule. However, the BIG-IP system cannot use the packet filter rule until you have enabled the Packet Filter feature. For more information, see **Enabling packet filtering**, on page 11-3.*

2. On the menu bar, click **Rules**.
   A list of any existing packet filter rules displays.

3. In the upper-right corner of the screen, click **Create**.
   The New Packet Filter Rule screen opens.

4. Configure all settings. For more information, see *Configuring settings for packet filter rules*, following, and *Creating a filter expression*, on page 11-10.

5. Click **Finished**.

Configuring settings for packet filter rules

You can configure a number of different settings when you create a packet filter rule. Table 11.3 lists and describes the settings that you can configure. Following the table are sections that provide more detail on each setting.

Setting	Description	Default Value
Name	Specifies a unique name for the packet filter.	No default value
Order	Specifies a number that you assign to a rule, which determines when the packet filter is processed. Low numbers take priority over higher ones.	No default value
Action	Specifies the action that BIG-IP system should take when a match is found. Possible values are: **Accept**, **Discard**, **Reject**, and **Continue**.	**Accept**

Table 11.3 *Configuration settings for a packet filter rule*

Setting	Description	Default Value
Rate Class	Lists one or more existing rate classes that you assign to the packet filter. This setting applies only when you have enabled the rate shaping feature. For more information on rate classes, see the *Configuration Guide for Local Traffic Management*.	**None**
Apply to VLAN	Specifies the incoming VLAN on which the BIG-IP system should search for matches.	*** ALL VLANS**
Logging	Action that the BIG-IP system takes to record every match that it finds.	**Disabled**

Table 11.3 *Configuration settings for a packet filter rule*

Specifying a name

Using the **Name** setting, you can specify a unique name for the packet filter rule. This setting is required.

Specifying the order of packet filter rules

You use the **Order** setting to specify the order in which you want the BIG-IP system to apply existing packet filter rules. This setting is required.

Possible values for this setting are:

- **First**
  Select this value if you want this packet filter rule to be the first rule that the BIG-IP system applies.
- **Last**
  Select this value if you want this packet filter rule to be the last rule that the BIG-IP system applies.
- **After**
  Select this value, and then select a packet filter rule from the list, if you want the system to apply this packet filter after the packet filter that you select from the list. Note that this setting is most useful when you have more than three packet filter rules configured.

Specifying an action

When a packet matches the criteria that you have specified in a packet filter rule, the BIG-IP system can take a specific action. You define this action using the **Action** setting.

You can choose one of these actions:

- **Accept**
  Select **Accept** if you want the system to accept the packet, and stop processing additional packet filter rules, if any exist. This is the default setting.

- **Discard**
  Select **Discard** if you want the system to drop the packet, and stop processing additional packet filter rules, if any exist.
- **Reject**
  Select **Reject** if you want the system to drop the packet, and also send a rejection packet to the sender, indicating that the packet was refused. Note that the behavior of the system when you select the **Reject** action depends on how you configured the general packet filter **Options** property **Send ICMP Error on Packet Reject**.
- **Continue**
  Select **Continue** if you simply want the system to acknowledge the packet for logging or statistical purposes. Setting the **Action** value to **Continue** does not affect the way that the BIG-IP system handles the packet; the system continues to evaluate traffic matching a rule, starting with the next packet filter rule in the list.

Assigning a rate class

Using the **Rate Class** setting, you can assign a rate class to traffic that matches the criteria defined in a packet filter rule. Note that this setting applies only when you have the rate shaping feature enabled.

The default value for this setting is **None**. If you previously created rate classes using the rate shaping feature, you can choose one of those rate classes from the **Rate Class** list.

For more information on rate shaping, see the ***Configuration Guide for Local Traffic Management***.

Specifying one or more VLANs

You use the **Apply to VLAN** setting to display a list of VLANs and then select a VLAN or VLAN group name. Selecting a VLAN from the list means that the packet filter rule filters ingress traffic from that VLAN only. For example, if you select the value ***All VLANS**, the BIG-IP system applies the packet filter rule to all traffic coming into the BIG-IP system.

Similarly, if you select the VLAN **internal**, the BIG-IP system applies the packet filter rule to traffic from VLAN **internal** only. The default value is ***All VLANS**.

If you select the name of a VLAN group instead of an individual VLAN, the packet filter rule applies to all VLANs in that VLAN group.

Enabling or disabling logging

If you want to generate a log message each time a packet matches a rule, you can enable logging for the packet filter rule. With this configuration, you can then display the Logging screen in the Configuration utility and view events related to packet filtering. For more information on logging packet filter events, see Chapter 17, *Logging BIG-IP System Events*.

Creating a filter expression

To match incoming packets, the BIG-IP system must use a filter expression. A ***filter expression*** specifies the criteria that you want the BIG-IP system to use when filtering packets. For example, the BIG-IP system can filter packets based on the source or destination IP address in the header of a packet.

Using the Configuration utility, you can create a filter expression in either of two ways:

- You can write your own expression, using a **Filter Expression** box.
- You can specify a set of criteria (such as source or destination IP addresses) that you want the BIG-IP system to use when filtering packets. When you use this method, the BIG-IP system builds a filter expression for you.

Figure 11.4 lists and describes the Filter Expression settings that you can configure when you want the BIG-IP system to build a filter expression. Note that some of these settings appear on the screen only if you configure other settings in a certain way.

Setting	Description	Default Value
Filter Expression Method	Specifies the manner in which you want to create the actual packet filter rule. Possible values are **Build Expression** or **Enter Expression Text**.	**Build Expression**
Protocols	Specifies that the BIG-IP system is to filter packets received from the specified protocols. If you select **Any**, the system filters packets from any protocol. If you select **Restrict to any in list**, the system filters packets from the specified protocols only.	**Any**
Protocol List	Specifies the protocols to which you want the packet filter to apply. You use the Move buttons (<< and >>) to create or modify the list.	No default value
Source Hosts and Networks	Specifies the source hosts and source networks to which you want the packet filter to apply. If you select **Any**, the system filters packets from any source host or source network. If you select **Restrict to any in list**, the system filters packets from the specified source addresses only.	**Any**
Source Hosts and Networks List	Specifies the source addresses to which you want the packet filter to apply. You use the Move buttons (<< and >>) to create or modify the list.	No default value
Destination Hosts and Networks	Specifies the destination hosts and destination networks to which you want the packet filter to apply. If you select **Any**, the system filters packets from any destination host or destination network. If you select **Restrict to any in list**, the system filters packets from the specified destination addresses only.	**Any**
Destination Hosts and Networks List	Specifies the destination addresses to which you want the packet filter to apply. You use the Move buttons (<< and >>) to create or modify the list.	No default value

Table 11.4 *Filter Expression settings for a packet filter rule*

Setting	Description	Default Value
Destination Port	Specifies the destination hosts ports to which you want the packet filter to apply. If you select **Any**, the system filters packets from any destination port. If you select **Restrict to any in list**, the system filters packets from the specified destination ports.	**Any**
Destination Port List	Specifies the destination ports to which you want the packet filter to apply. You use the Move buttons (<< and >>) to create or modify the list.	No default value

Table 11.4 *Filter Expression settings for a packet filter rule*

You can have as many rules as you want, limited only by the available memory. Of course, the more statements you have, the more challenging it is to understand and maintain your packet filters.

Managing packet filter rules

Once you have created packet filter rules, you can list them, view or modify their settings, or delete them. You can also view statistics related to packet filters.

Viewing the list of packet filter rules

Using the Configuration utility, you can view a list of any packet filter rules previously created. The screen that lists existing packet filter rules shows the following information for each packet filter rule:

- The order in which the system applies the packet filter rule
- The name of the packet filter rule
- The action that the BIG-IP system takes based on the criteria defined in the packet filter rule
- The VLAN traffic to which the packet filter rule applies
- If rate shaping is enabled, the rate class that applies to traffic that matches the criteria defined in the packet filter rule
- The logging state (enabled or disabled)

For information on creating packet filter rules, see *Configuring settings for packet filter rules*, on page 11-7.

Use the following procedure to view a list of packet filter rules.

To view the list of packet filter rules

1. On the Main tab of the navigation pane, expand **Network,** and click **Packet Filters**.
   This displays properties for global packet filtering, if packet filtering is enabled.
2. On the menu bar, click **Rules.**
   This displays the list of all existing packet filters.

Viewing or modifying packet filter rule settings

You can use the Configuration utility to view or modify the current settings of a packet filter rule. For information on how to initially enable packet filtering and configure the settings for a packet filter rule, see *Creating packet filter rules*, on page 11-7.

To view or modify packet filter settings

1. On the Main tab of the navigation pane, expand **Network,** and click **Packet Filters**.
   This displays properties for global packet filtering, if packet filtering is enabled.
2. On the menu bar, click **Rules.**
   This displays the list of all existing packet filters.
3. Click a packet filter name in the list.
   This displays the settings for that packet filter.
4. Retain or modify any settings.
5. Click **Update**.

Deleting a packet filter rule

You can use the Configuration utility to delete a packet filter rule.

To delete a packet filter rule

1. On the Main tab of the navigation pane, expand **Network,** and click **Packet Filters**.
   This displays properties for global packet filtering, if packet filtering is enabled.
2. On the menu bar, click **Rules.**
   This displays the list of all existing packet filters.
3. Locate a packet filter name in the list.
4. To the left of the name, check the Select box.

5. At the bottom of the screen, click **Delete**.
   A confirmation message appears.
6. Click **Delete** again.

Viewing statistics for packet filters

The Configuration utility displays a number, known as a ***hit count***, that increments each time a packet matches the packet filter rule.

To view packet filter statistics

1. On the Main tab of the navigation pane, expand **Network,** and click **Packet Filters**.
   This displays properties for global packet filtering, if packet filtering is enabled.
2. On the menu bar, click **Statistics**.
   This displays the main Statistics screen in the Configuration utility.
3. Using the **Data Format** list, select either **Normalized** or **Unformatted**.
   This displays packet filter statistics, in the chosen display mode.

12

Configuring Spanning Tree Protocols

- Introducing spanning tree protocols
- Configuring global spanning tree properties
- Managing spanning tree instances
- Configuring interfaces for spanning tree

Introducing spanning tree protocols

On networks that contain redundant paths between layer 2 devices, a common problem is bridging loops. Bridging loops occur because layer 2 devices do not create boundaries for broadcasts or packet floods. Consequently, layer 2 devices can use redundant paths to forward the same frames to each other continuously, eventually causing the network to fail.

To solve this problem, the BIG-IP system supports a set of industry-standard, layer 2 protocols known as spanning tree protocols. ***Spanning tree protocols*** block redundant paths on a network, thus preventing bridging loops. If a blocked, redundant path is needed later because another path has failed, the spanning tree protocols clear the path again for traffic. The spanning tree protocols that the BIG-IP system supports are Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).

Central to the way that spanning tree protocols operate is the use of bridge protocol data units (BPDUs). When you enable spanning tree protocols on layer 2 devices on a network, the devices send ***BPDUs*** to each other, for the purpose of learning the redundant paths and updating their L2 forwarding tables accordingly, electing a root bridge, building a spanning tree, and notifying each other about changes in interface status.

◆ **Note**

Throughout this chapter, the term ***bridge*** *refers to a layer 2 device such as a switch, bridge, or hub.*

Spanning tree protocol types

The BIG-IP system supports three different spanning tree protocols: STP, RSTP, and MSTP. Table 12.1 lists the protocols and their IEEE specifications. Following the table is a brief summary of each protocol.

Protocol Name	IEEE Specification
Spanning Tree Protocol (STP)	802.1D-1998
Rapid Spanning Tree Protocol (RSTP)	802.1w, 802.1t, and 802.1D-2004
Multiple Spanning Tree Protocol (MSTP)	802.1s

Table 12.1 *The spanning tree protocols that the BIG-IP system supports*

The STP protocol

STP is the original spanning tree protocol, designed to block redundant paths as a way to prevent bridging loops. The STP algorithm creates one, and only one, spanning tree for the entire network. A ***spanning tree*** is a logical tree-like depiction of the bridges on a network and the paths that connect them.

Because STP is unable to recognize VLANs and usually exhibits poor performance overall, STP is not the preferred spanning tree protocol to use in VLAN-rich environments. However, all participating interfaces in the spanning tree must use the same spanning tree protocol at any given time. Thus, when you have legacy bridges in your environment that are running STP, interfaces on the BIG-IP system must have the ability to automatically degrade to STP. For more information on protocol degradation, see *Using spanning tree with legacy bridges*, on page 12-3.

Because STP has no knowledge of VLANs, you can have only one spanning tree instance on the BIG-IP system when using STP. For more information on spanning tree instances, see *Managing spanning tree instances*, on page 12-10.

The RSTP protocol

RSTP is an enhancement to STP, and was designed specifically to improve spanning tree performance. Like STP, RSTP can create only one spanning tree (instance **0**), and therefore cannot take VLANs into account when managing redundant paths. However, RTSP's performance improvements generally make it preferable to STP in non-VLAN environments.

In the case where legacy RSTP bridges are on the network, BIG-IP system interfaces running MSTP can degrade to RSTP, just as they can degrade to STP. For more information on protocol degradation, see *Using spanning tree with legacy bridges*, on page 12-3.

Like STP, RSTP allows only one spanning tree instance on the BIG-IP system. For more information on spanning tree instances, see *Managing spanning tree instances*, on page 12-10.

The MSTP protocol

MSTP is an enhancement to RSTP and is the preferred spanning tree protocol for the BIG-IP system. MSTP is specifically designed to understand VLANs and VLAN tagging (specified in IEEE 802.1q). Unlike STP and RSTP, which allow only one spanning tree instance per system, MSTP allows multiple spanning tree instances. Each instance corresponds to a spanning tree, and can control one or more VLANs that you specify when you create the instance. Thus, for any BIG-IP system interface that you assigned to multiple VLANs, MSTP can block a path on one VLAN, while still keeping a path in another VLAN open for traffic. Neither STP nor RSTP has this capability.

A unique feature of MSTP is the concept of spanning tree regions. A ***spanning tree region*** is a logical set of bridges on the network that share the same values for certain MSTP configuration settings. These configuration settings are: The MSTP configuration name, the MSTP configuration number, the instance numbers, and the VLAN members of each instance. When the values of these settings are identical on two or more bridges, the spanning tree algorithm considers these bridges to constitute an MSTP region. An ***MSTP region*** indicates to the spanning tree algorithm that it can use MSTP for all bridges in that region, and thus take VLANs into account when blocking and unblocking redundant paths.

You do not explicitly create a region. The spanning tree algorithm automatically groups bridges into regions, based on the values you assign to the MSTP configuration name, revision number, instance numbers, and instance members.

MSTP can only operate on bridges that are within a region. However, if the BIG-IP system connects to a bridge in a different MSTP region or outside of an MSTP region, the system still participates in spanning tree. In this case, the system is part of the spanning tree instance **0**, also known as the Common and Internal Spanning Tree (CIST).

◆ **Note**

BIG-IP systems released prior to version 9.0 do not support MSTP.

Using spanning tree with legacy bridges

A key concept about spanning tree protocols on the BIG-IP system is the concept of protocol degradation. ***Protocol degradation*** occurs when the spanning tree mode on the BIG-IP system is set to MSTP or RSTP, but the system detects legacy bridges (that is, bridges running an older protocol type) on the network. In this case, the BIG-IP system automatically degrades the spanning tree protocol that is running on each applicable interface to match the protocol running on the legacy device.

For example, suppose you set the BIG-IP system to run in MSTP mode. Later, if a bridge running STP is added to the network, the BIG-IP system will detect the legacy device and automatically degrade the protocol running on the BIG-IP system interfaces from MSTP to STP. The mode is still set to MSTP, but the interfaces actually run STP.

If the legacy device is later removed from the network, you can choose, for each BIG-IP system interface, to manually reset the spanning tree protocol back to MSTP.

The basic principle of protocol degradation is that each BIG-IP system interface in a spanning tree runs the oldest protocol that the system detects on the layer 2 devices of the network. Thus, if a legacy bridge running STP is added to the network, BIG-IP system interfaces running MSTP or RSTP degrade to STP. Similarly, if a legacy bridge is running RSTP (and no bridges are running STP), interfaces running MSTP degrade to RSTP.

Note that when a bridge running MSTP must degrade to RSTP, the spanning tree algorithm automatically puts the degraded bridge into a separate MSTP region.

Configuration overview

Regardless of which spanning tree protocol you choose to use, the BIG-IP system offers a complete set of default configuration settings. Except for choosing a preferred spanning tree protocol to use, there are very few configuration settings that you need to modify to use the spanning tree feature effectively.

When you configure spanning tree on a BIG-IP system, you must first decide which protocol, or mode, you want to enable. Because MSTP recognizes VLANs, using MSTP is preferable for the BIG-IP system. However, all bridges in a network environment that want to use spanning tree must run the same spanning tree protocol. If a legacy bridge running RSTP or STP is added to the network, the BIG-IP system must switch to that same protocol.

Fortunately, you do not need to continually reconfigure the BIG-IP system spanning tree mode whenever a legacy bridge is added to the network. Instead, a BIG-IP system interface can detect the addition of a legacy bridge and automatically fall back to either RSTP or STP mode. If the legacy bridge is later removed from the network, you can use the Configuration utility to manually reset the interface back to running MSTP. For more information on legacy bridges, see *Using spanning tree with legacy bridges*, on page 12-3.

Once you have enabled a spanning tree mode, you can configure a set of global options. These options are the same options that are defined in the IEEE standards for the spanning tree protocols. While you can use the default settings in most cases, a few settings require user input. For more information, see *Configuring global spanning tree properties*, on page 12-5.

Configuring global spanning tree properties

There are several properties you can configure on the BIG-IP system that affect the behavior of all spanning tree protocols. These global properties apply to all spanning instances and all network interfaces. In most cases, you can use the default values for these properties. Table 12.2 lists these global properties.

Property	Description	Default Value
Mode	Specifies the protocol you want to use or not use. Possible settings are: **Disabled**, **Pass Through**, **STP**, **RSTP**, **MSTP**.	**Pass Through**
Hello Time	Specifies, in seconds, how often the system broadcasts HELLO frames to other members of the spanning tree.	**2**
Maximum Age	Specifies, in seconds, the length of time for which spanning tree information from other bridges is considered valid.	**20**
Forward Delay	Specifies, in seconds, the length of time for which an interface is blocked from forwarding network traffic after the spanning tree topology has been modified. This property is more useful for STP than RSTP or MSTP.	**15**
Transmit Hold Count	Specifies the maximum number of spanning tree frames the system can transmit on a port within the Hello Time interval.	**6**
MSTP Configuration Name	For MSTP only, specifies the name of the spanning tree configuration. All bridges with the same MSTP configuration name, MSTP configuration revision number, instance numbers, and instance members are considered to be in the same MSTP region.	MAC address of lowest-numbered interface
MSTP Configuration Revision	For MSTP only, specifies the revision level of an MSTP configuration.	**0**
MSTP Maximum Hops	For MSTP only, specifies the maximum number of hops that a spanning tree frame can traverse before it is discarded.	**20**

Table 12.2 *Global spanning tree properties*

Use the following procedure to configure global spanning tree properties. For detailed information on each property, see these sections:

- *Specifying the spanning tree mode*, on page 12-6
- *Configuring global timers*, on page 12-7
- *Specifying the Transmit Hold Count option*, on page 12-8
- *Configuring MSTP-specific global properties*, on page 12-8

To configure global spanning tree properties

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This opens the Spanning Tree screen.
2. On the menu bar, click **Options**.
   This displays the screen for configuring global spanning tree properties.
3. Configure the properties as needed.
   For information on each property, see the following sections.
4. Click **Update**.

Specifying the spanning tree mode

The **Mode** option specifies the particular spanning tree protocol that you want to use on the BIG-IP system. The default value is **Pass Through**. The possible values are:

- **Disabled**
  Specifies that when the BIG-IP system receives spanning tree frames (BPDUs), it discards the frames.
- **Pass Through**
  Specifies that when the BIG-IP system receives spanning tree frames (BPDUs), it forwards them to all other interfaces. This is the default setting. When you use **Pass Through** mode, the BIG-IP system is transparent to spanning tree BPDUs. When set to **Pass Through** mode, the BIG-IP system is not part of any spanning tree. Note that **Pass Through** mode is not part of the IEEE spanning tree protocol specifications.
- **STP**
  Specifies that the BIG-IP system handles spanning tree frames (BPDUs) in accordance with the STP protocol. This mode allows for legacy systems on the network. For more information on STP, see *Introducing spanning tree protocols*, on page 12-1.
- **RSTP**
  Specifies that the BIG-IP system handles spanning tree frames (BPDUs) in accordance with the RSTP protocol. For more information RSTP, see *Introducing spanning tree protocols*, on page 12-1.
- **MSTP**
  Specifies that the BIG-IP system handles spanning tree frames (BPDUs) in accordance with the MSTP protocol. For more information MSTP, see *Introducing spanning tree protocols*, on page 12-1.

Important

If you select MSTP mode, additional options appear on the screen.

When you set the mode to MSTP or RSTP, and a legacy bridge running STP is subsequently added to the spanning tree, the applicable BIG-IP system interface automatically changes to running STP. However, you can manually reset an interface to resume operation in RSTP or MSTP mode if the legacy bridge is later removed from the spanning tree. For information on detecting the protocol version, see *Configuring interfaces for spanning tree*, on page 12-17.

Configuring global timers

All three spanning tree protocols, have the same three global timer values that you can specify: **Hello Time**, **Maximum Age**, and **Forward Delay**.

Specifying the Hello Time option

When you change the value of the **Hello Time** option, you change the time interval, in seconds, that the BIG-IP system transmits spanning tree information (through BPDUs) to adjacent bridges in the network. The default value for this option is **2**.

◆ **WARNING**

Although valid values are in the range of 1 to 10 seconds, we highly recommend that you use the default value (2 seconds). This value is optimal for almost all configurations.

Note that when running RSTP, you must maintain the following relationship between the **Maximum Age** and **Hello Time** options:

```
Maximum Age >= 2 * (Hello Time + 1)
```

Specifying the Maximum Age option

When you change the value of the **Maximum Age** option, you change the amount of time, in seconds, that spanning tree information received from other bridges is considered valid. The default value is **20**, and the valid range is 6 to 40.

Note that when running RSTP, you must maintain the following relationships between the **Maximum Age** and the **Hello Time** and **Forward Delay** options:

```
Maximum Age >= 2 * (Hello Time + 1)
Maximum Age <= 2 * (Forward Delay - 1)
```

Specifying the Forward Delay option

Primarily used for STP, the **Forward Delay** option specifies the amount of time, in seconds, that the system blocks an interface from forwarding network traffic when the spanning tree algorithm reconfigures a spanning tree. The default value is **15**, and the valid range is 4 to 30.

This option has no effect on the BIG-IP system when running in RSTP or MSTP mode, as long as all bridges in the spanning tree use the RSTP or MSTP protocol. However, if the addition of legacy STP bridges causes neighboring bridges to fall back to running the STP protocol, then the spanning tree algorithm uses the **Forward Delay** option when reconfiguring the spanning tree.

Note that when running RSTP, you must maintain the following relationship between the **Forward Delay** and **Maximum Age** options:

```
Maximum Age <= 2 * (Forward Delay - 1)
```

Specifying the Transmit Hold Count option

When you change the value of the **Transmit Hold Count** option, you change the maximum number of spanning tree frames (BPDUs) that the system can transmit on a port within the **Hello Time** interval. This setting ensures that the spanning tree frames do not overload the network, even in unstable network conditions. The default value is **6**, and the valid range is 1 to 10.

Configuring MSTP-specific global properties

If you are running MSTP, you can configure three additional global properties: An MSTP configuration name, an MSTP configuration revision, and a maximum hop number.

Specifying an MSTP configuration name

Applicable to MSTP only, the **MSTP Configuration Name** setting represents a global name that you assign to all bridges in a spanning tree region. A ***spanning tree region*** is a group of bridges with identical MSTP configuration names and MSTP configuration revision levels, as well as identical assignment of VLANs to spanning tree instances.

All bridges in the same region must have this same configuration name. The name must contain from 1 to 32 characters. This option only appears on the screen when you set the **Mode** property to **MSTP**.

For more information on MSTP regions, see *The MSTP protocol*, on page 12-2.

Specifying an MSTP configuration revision

Applicable to MSTP only, the **MSTP Configuration Revision** setting represents a global revision number that you assign to all bridges in a spanning tree region. All bridges in the same region must have this same configuration revision number. The default value is **0**. You can type any value between 0 and 65535. This option only appears on the screen when you set the **Mode** property to **MSTP**.

For more information on MSTP regions, see *The MSTP protocol*, on page 12-2.

Specifying a maximum hop number

Applicable to MSTP only, this global property specifies the maximum number of hops that a spanning tree frame (BPDU) can traverse before it is discarded. The default value is **20**. You can specify a value between 1 and 255. This option only appears on the screen when you set the **Mode** property to **MSTP**.

Managing spanning tree instances

By default, the spanning tree protocol STP is enabled on all of the interfaces of the BIG-IP system. The default spanning tree configuration includes a single spanning tree instance, named **0**. A ***spanning tree instance*** is a discrete spanning tree for a network. While STP and RSTP allow only one spanning tree instance (instance **0**), MSTP allows you to create multiple spanning tree instances, to manage redundant paths for specific VLANs on the network.

When running MSTP, instances that you create have instance members. An ***instance member*** is a VLAN that you assign to an instance when you create that instance. You can assign as many or as few members to an instance as you deem necessary. By default, all VLANs on the BIG-IP system are members of instance **0**.

If you create an instance and attempt to add a VLAN that is already a member of another instance, the BIG-IP system deletes the VLAN from the existing instance and adds the VLAN to the new instance.

Each instance name must be a numeric value that you assign when you create the instance.

When you manage a spanning tree instance, you can:

- View a list of instances
- Create an instance (MSTP only)
- Modify instance properties
- Delete an instance or its members (MSTP only)

Viewing a list of spanning tree instances

You can view a list of existing spanning tree instances using the Configuration utility. For STP and RSTP, the only instance in the list is instance **0**. For MSTP, the list shows instance **0**, plus any other instances that you have explicitly created. For information on creating a spanning tree instance, see *Configuring interfaces for spanning tree*, on page 12-17.

When you view a list of instances, you can see the following information for each instance:

- The name of the instance
- The bridge priority number
- The MAC address of the root bridge
- The MAC address of the regional root bridge
- The number of instance members

To view a list of spanning tree instances

On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**. This opens the Spanning Tree screen, which lists all existing instances.

Creating a spanning tree instance (MSTP-only)

The STP and RSTP protocols allow only one spanning tree instance, instance **0**, which the BIG-IP system creates automatically when you enable spanning tree. When running STP or RSTP, you can modify the properties of instance **0**, but you cannot create additional instances. For information on modifying the properties of an instance, see *Viewing and modifying a spanning tree instance*, on page 12-15.

When you are running MSTP, however, the MSTP algorithm can explicitly create instances. The reason that you can create instances is that MSTP recognizes VLANs. By creating an instance and assigning one or more VLANs to it, you can control bridge loops and redundant paths within those VLANs.

For example, suppose you have two interfaces. One interface is assigned to VLAN A, while the other interface is assigned to VLANs A and B. If you are using the STP or RSTP protocol, both of which disregard VLANs, the protocol might block traffic for both VLANs, as shown in Figure 12.1.

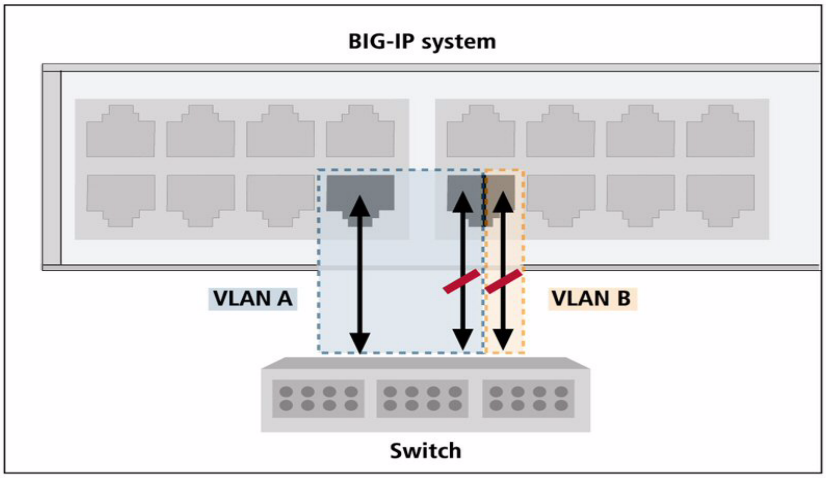


Figure 12.1 *Using STP or RSTP to block redundant paths*

By contrast, the MSTP protocol can make blocking decisions on a per-VLAN basis. In our example, on the interface that carries traffic for two VLANs, you can block traffic for VLAN A, but leave a path open for VLAN B traffic. This is shown in Figure 12.2, on page 12-12.

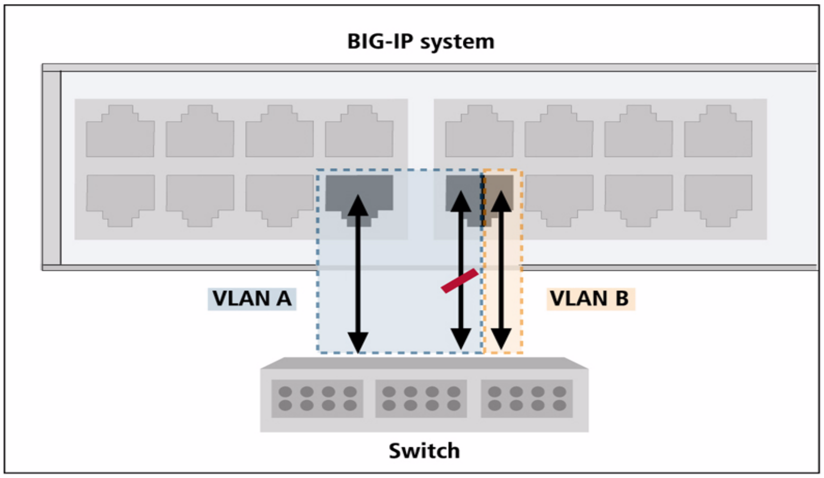


Figure 12.2 Using MSTP to block redundant paths

Because all BPDUs exchanged within a region always reference instance 0, instance 0 is active on all interfaces. This, in turn, can cause blocking problems. To avoid this, make sure that each VLAN on a BIG-IP system is a member of an instance that you explicitly create, rather than a member of instance 0 only. For example, suppose you create the following:

- Instance 1 with VLAN A as a member, where VLAN A is associated with interface 1.2
- Instance 2 with VLAN B as a member, where VLAN B is associated with interface 1.4

In this case, neither interface will be blocked, because the BPDUs sent from each interrace reference a unique instance (either instance 1 or instance 2).

Table 12.3 shows the properties that you configure when you create or modify a spanning tree instance.

Property	Description	Default Value
Instance ID	Specifies a numeric identification for the instance. This number can be between 1 and 255.	No default value
Bridge Priority	Specifies the spanning tree bridge priority for the instance.	**61440**
VLANs	For MSTP only, specifies the VLANs that you want to be members of the instance.	**external** and **internal**

Table 12.3 *Configurable properties of a spanning tree instance*

Use the following procedures to create a spanning tree instance. For more information on each property that you configure, see the sections that follow the procedures.

◆ **Important**

*From the Configuration utility screen that lists existing spanning tree instances, you create instances using a special **Create** button. This **Create** button appears only when you are running MSTP. If you are running MSTP, but no **Create** button appears on the screen, your BIG-IP hardware platform does not support MSTP. For more information on creating a spanning tree instance, see **To create a spanning tree instance (MSTP only)**, following.*

◆ **Tip**

*Because all BPDUs exchanged within a region always reference instance **0**, thereby causing instance **0** to be active on all interfaces, unwanted blocking problems can occur. To avoid this, make sure that each VLAN on a BIG-IP system is a member of an instance that you explicitly create, rather than a member of instance **0** only.*

To create a spanning tree instance (MSTP only)

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This opens the Spanning Tree screen, which lists all existing spanning tree instances.

2. In the upper right corner of the screen, click **Create**.
   This displays the properties for that instance.

   ***Note:** If you do not see a **Create** button, then either the global **Mode** property is not set to **MSTP**, or your BIG-IP system hardware platform does not support MSTP.*

3. In the **Instance ID** box, type an instance identification number.

4. From the **Bridge Priority** list, select a bridge priority or retain the default value.
   For more information, see *Selecting a bridge priority*, on page 12-14.

5. For the **VLANs** property, use the Move button (**<<**) to add members to the instance, or retain the default members.

   ***Note:** If no VLANs appear in the **Available** box, or you need more information, see **Adding VLANs to an instance**, on page 12-14.*

6. Click **Finished**.

◆ **Note**

Once you create a spanning tree instance, it is automatically enabled. You do not need to explicitly enable it.

Assigning an instance ID

When you configure the **Instance ID** setting, you specify a numeric value for the instance, in the range of 1 to 255. The reason that instance names must be numeric is to handle the requirement that all cooperating bridges agree on the assignment of VLANs to instance IDs. Using numeric values instead of names makes this requirement easier to manage.

Selecting a bridge priority

The bridge in the spanning tree with the lowest relative priority becomes the root bridge. A ***root bridge*** represents the root of a spanning tree, and is responsible for managing loop resolution on the network. We recommend that you configure this setting so that the BIG-IP system never becomes the root bridge. For this reason, the default value for the **Bridge Priority** setting is **61440**, the highest value that you can select. Note that a bridge priority must be in increments of 4096.

Adding VLANs to an instance

If you are running MSTP, you can add members to a spanning tree instance. An ***instance member*** is a VLAN. You add members to an instance by associating one or more VLANs with the instance. The interfaces or trunks associated with each VLAN automatically become part of the spanning tree corresponding to that instance.

For two or more bridges to operate in the same spanning tree, all of those bridges must be in the same region, and therefore must have the same instance numbers, instance members, and VLAN tags.

For example, if a bridge has instance **1**, with two VLAN members whose tags are **1000** and **2000**, then any other bridges that you want to operate in that spanning tree must also have instance **1** with two VLAN members whose tags are **1000** and **2000**. For more information on MSTP regions, see *The MSTP protocol*, on page 12-2.

A particular VLAN cannot be associated with more than one spanning tree instance. For example, if you have two instances named **0** and **1**, you can only associate VLAN **external** with one of those instances, not both. Therefore, before creating an instance, verify that each VLAN you intend to associate with the instance is not a member of another instance.

◆ **Tip**

*If no VLANs appear in the **Available** box when creating an instance, it is likely that all VLANs on the BIG-IP system are members of other instances. You can verify this by viewing the members of other instances. For more information, see **Viewing and modifying a spanning tree instance**, following.*

Viewing and modifying a spanning tree instance

Using the Configuration utility, you can view and modify properties of any instance, including instance **0**. If you are running MSTP, you can modify the **Bridge Priority** and **VLANs** properties. If you are running RSTP or STP, you can modify only the **Bridge Priority** property. In no case can you modify the instance ID.

The procedure for viewing and modifying the properties of an instance follows. For information on the **Bridge Priority** and **VLANs** properties, see *Selecting a bridge priority*, on page 12-14 and *Adding VLANs to an instance*, on page 12-14.

To view and modify properties of an instance

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This displays the list of spanning tree instances.
2. In the Name column, click an instance number.
   This displays the properties for that instance.
3. Make any modifications that are available for the particular spanning tree protocol you are using (STP, RSTP, or MSTP).
4. Click **Update**.

Deleting a spanning tree instance or its members (MSTP-only)

If you are running MSTP, you might have explicitly created some spanning tree instances. If so, you can delete any spanning tree instance except instance **0**.

You can also remove VLAN members from an instance. When you remove a VLAN from an instance, the VLAN automatically becomes a member of instance **0**. (By default, instance **0** includes any VLAN that is not a member of another instance.)

If you remove all members from an instance, the BIG-IP system automatically deletes the instance.

◆ **Note**

*If you are running RSTP or STP, you cannot delete instance **0** or remove members from it.*

To delete a spanning tree instance

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This displays the list of spanning tree instances.
2. In the Name column, locate the instance number.
3. To the left of the instance number, check the Select box.

4. Click **Delete**.
   A confirmation message appears.
5. Click **Delete.**

To delete members from a spanning tree instance

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This displays the list of spanning tree instances.
2. In the Name column, click an instance name.
   This displays the properties for that instance.
3. For the **VLANs** property, use the Move button (>>) to delete members from the instance.
4. Click **Update**.

Configuring interfaces for spanning tree

Some of the configuration tasks you perform when managing a spanning tree protocol pertain to BIG-IP system interfaces. The interface-related tasks you perform are:

- Configuring settings on each interface that is to be part of the spanning tree
- Managing interfaces per spanning tree instance

Configuring spanning tree settings on an interface

For each interface on the BIG-IP system, there are several STP-related settings that you can configure. Table 12.4 lists these settings.

Setting	Description	Default Value
STP	Specifies whether the interface can participate in the spanning tree. By default, this setting is enabled on all BIG-IP system interfaces.	Enabled
STP Link Type	Specifies the link type so that STP uses the correct optimizations for the interface. Possible values are **p2p**, **Shared**, and **Auto**.	**Auto**
STP Edge Port	Specifies, when checked, that the interface connects to an end station instead of another spanning tree bridge.	Enabled
STP Edge Port Detection	Specifies, when checked, that the system automatically determines the edge port status of the interface.	Enabled
STP Protocol Detection	Resets the interface back to using the RSTP or MSTP protocol after a legacy bridge has been removed. You must manually reset an interface whenever a legacy bridge is removed from the network.	No default value

Table 12.4 *Configuration settings for an interface*

Use the following procedure to configure the spanning tree settings of an individual interface. For detailed information on each setting, see the sections following the procedure.

◆ **Note**

There are additional interface properties and settings that apply to specific spanning tree instances only. For more information, see ***Managing interfaces for a specific instance****, on page 12-20.*

To configure spanning tree settings for an interface

1. On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**.
   This displays the list of the interfaces on the BIG-IP system.
2. In the Name column, click an interface name.
   This displays the general properties of that interface, as well as some configuration settings.
3. In the STP Configuration area, configure the settings as needed.
   For information on each setting, see the following sections.
4. Click **Update**.

Enabling and disabling Spanning Tree

When you check the box for the **STP** setting, you are specifying that the interface can become part of a spanning tree. Once the interface becomes part of the spanning tree, the spanning tree protocol takes control of all learning and frame forwarding on that interface.

If you disable this setting, the spanning tree protocol treats the interface as non-existent, and does not send BPDUs to that interface. Also, the interface, and not the spanning tree protocol, controls all learning and frame forwarding for that interface.

Note that you can also enable or disable spanning tree for a trunk. If spanning tree is enabled on the reference link of a trunk (that is, the lowest-numbered interface of the trunk), then spanning tree is automatically enabled on that trunk. To disable spanning tree for a trunk, simply disable spanning tree on the reference link.

Specifying the STP link type

When you specify an STP link type, you ensure that STP uses the correct optimizations for the interface. Possible values are:

- **auto**
  When you set the STP link type to **auto**, the BIG-IP system determines the spanning tree link type, which is based on the **Active Duplex** interface property.
- **p2p**
  When you set the STP link type to **p2p**, the BIG-IP system uses the optimizations for point-to-point spanning tree links. Point-to-point links connect two spanning tree bridges only. For example, a point-to-point link might connect a 10 Gigabit link to another bridge. For point-to-point links, the **Active Duplex** property interface should be set to **full**. Note that **p2p** is the only valid STP link type for a trunk.
- **shared**
  When you set the STP link type to **shared**, the BIG-IP system uses the optimizations for shared spanning tree links. Shared links connect two or

more spanning tree bridges. For example, a shared link might be a 10 Megabit hub. Note that for shared links, the **Active Duplex** interface property should be set to **half**.

Enabling and disabling an STP edge port

When you enable the **STP Edge Port** setting, you are explicitly designating the interface as an edge port. An ***edge port*** is an interface that connects to an end station rather than to another spanning tree bridge. The default setting is disabled (not checked).

If you would rather have the system automatically designate the interface as an edge port, you can enable the **STP Edge Port Detection** setting instead, described in the following section.

If you enable (check) the **STP Edge Port** setting and the interface subsequently receives STP, RSTP, or MSTP frames (BPDUs), the system disables the setting automatically, because only non-edge interfaces receive BPDUs.

Enabling and disabling detection of an STP edge port

When you enable the **STP Edge Port Detection** setting, the system determines whether the interface is an edge port, and if so, automatically designates the interface as an edge port. The system determines edge port status by monitoring the interface and verifying that it does not receive any incoming STP, RSTP, or MSTP frames (BPDUs).

If the system determines that the interface is not an edge port, but you enabled the **STP Edge Port** setting to explicitly designate the interface as an edge port, the system removes the edge port designation from the interface. No interface that receives BPDUs from a bridge can have edge port status, despite the values of the **STP Edge Port** and **STP Edge Port Detection** settings.

Resetting the spanning tree protocol

As described in *Configuring global spanning tree properties*, on page 12-5, the spanning tree algorithm automatically detects the presence of legacy STP bridges on the network, and falls back to STP mode when communicating with those bridges. Because legacy STP bridges do not send spanning tree BPDUs periodically in all circumstances, the BIG-IP system cannot detect when a legacy STP bridge has been removed from the network. Therefore, it is necessary to manually notify the BIG-IP system that the algorithm can switch to the RSTP or MSTP protocol again, whenever a legacy bridge has been removed.

You reset an interface using the **Reset** button for the **STP Protocol Detection** setting.

Managing interfaces for a specific instance

When you manage an interface for a specific spanning tree instance, you can:

- View a list of interfaces for an instance
- View instance-specific properties of an interface
- Configure instance-specific settings for an interface

Viewing a list of interface IDs for an instance

Using the Configuration utility, you can view a list of the interface IDs associated with a specific spanning tree instance.

If you are using MSTP, the interface IDs that appear in the list are the interfaces assigned to the VLANs that you specified when you created the instance. If you are using STP or RSTP, the interface IDs in the list are those that the BIG-IP system automatically assigned to instance **0**.

The list of interface IDs also displays the following information for each interface:

- The STP instance ID
- The priority
- The external path cost
- The port role

To view a list of interfaces for an instance

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This opens the Spanning Tree screen and displays a list of existing instances.
2. In the Name column, click an instance number.
   This displays the properties of that instance.
3. On the menu bar, click **Instance Interfaces**.
   This displays a list of the interfaces for that instance.

Viewing instance-specific properties of an interface

Once you have used the previous procedure to view the list of interfaces associated with a particular spanning tree instance, you can view the properties associated with that interface. Some of these properties are those that you configured using the Interfaces screen. Table 12.5 shows the per-instance interface properties that you can view.

Setting	Description	Default Value
Port Role	Indicates the spanning tree role of the interface (port) with regard to the spanning tree instance. The system determines the interface role automatically.	No default value
Port State	Indicates the manner in which the interface (port) processes any frames that are not spanning tree frames. The system determines the interface state automatically.	No default value

Table 12.5 *Viewable properties of a per-instance interface*

The following two sections describe the **Port Role** and **Port State** properties. For information on the other properties shown in Table 12.5, see *Configuring spanning tree settings on an interface*, on page 12-17.

Understanding the port roles

The **Port Role** property of a per-instance interface specifies the interface's role in the spanning tree instance. You cannot specify a value for this property; the BIG-IP system automatically assigns a role to the interface.

The BIG-IP system can assign one of the following roles to an instance interface:

- **Disabled**
  The interface has no active role in the spanning tree instance.
- **Root**
  The interface provides a path to a root bridge.
- **Alternate**
  The interface provides an alternate path to a root bridge, if the root interface is unavailable.
- **Designated**
  The interface provides a path away from the root bridge.
- **Backup**
  The interface provides an alternate path away from the root bridge, if an interface with a port role of **Designated** is unavailable. The **Backup** role assignment is rare.

Understanding port states

The **Port State** property of an interface specifies the way that the interface processes normal data packets. You cannot specify a value for this property; the BIG-IP system automatically assigns a state to the interface.

An interface can be in one of the following states at any given time:

- **Blocking**
  The interface disregards any incoming frames, and does not send any outgoing frames.
- **Forwarding**
  The interface passes frames as needed.
- **Learning**
  The interface is determining information about MAC addresses, and is not yet forwarding frames.

Configuring instance-specific settings for an interface

There are a few settings that you configure for an interface that only pertain to a specific instance. Table 12.6 lists and describes these settings.

Setting	Description	Default Value
Interface Priority	Specifies the interface's priority in relation to the other interfaces that are members of the spanning tree instance.	**128**
External Path Cost	Specifies the relative cost of sending traffic through the interface.	Depends on interface speed
Internal Path Cost	Specifies the relative cost of sending traffic through the interface to adjacent bridges within a spanning tree region.	Depends on interface speed

Table 12.6 *Configurable settings of an interface for a specific instance*

Use the following procedure to configure the settings of an interface for a specific instance. For detailed information on each setting, see the sections following the procedure.

To configure interface settings per instance

1. On the Main tab of the navigation pane, expand **Network**, and click **Spanning Tree**.
   This opens the Spanning Tree screen and displays a list of existing instances.
2. In the Name column, click an instance number.
   This displays the properties of that instance.
3. On the menu bar, click **Instance Interfaces**.
   This displays a list of the interfaces for that instance.

4. In the Name column, click an interface number.
   This displays properties and settings for that interface, for the relevant instance.
5. In the Configuration area, configure the settings.
   For information on these settings, see the following sections.
6. Click **Update**.

Selecting an interface priority

Each interface has an associated priority within a spanning tree instance. The relative values of the interface priorities affect which interfaces the system chooses to carry network traffic. Using the **Interface Priority** setting, you can select the interface's priority in relation to the other interfaces that are members of the spanning tree instance.

Typically, the system is more likely to select interfaces with lower numeric values to carry network traffic. A priority value that you assign to an interface can be in the range of **0** to **240**, in increments of 16. Thus, the value you assign to an interface can be **0**, **16**, **32**, **64**, and so on, up to **240**.

The default priority for an interface is **128**, the middle of the valid range.

Specifying path cost

Each interface has an associated path cost within a spanning tree instance. The ***path cost*** represents the relative cost of sending network traffic through that interface. When calculating the spanning tree, the spanning tree algorithm attempts to minimize the total path cost between each point of the tree and the root bridge. By manipulating the path costs of different interfaces, you can steer traffic toward paths that are either faster, more reliable, more economical, or have all of these qualities.

The value of a path cost can be in the range of **1** to **200,000,000**, unless you have legacy STP bridges. In that case, because some legacy implementations support a range of only **1** to **65535**, you should use this more restricted range when setting path costs on interfaces.

The default path cost for an interface is based on the maximum speed of the interface rather than the actual speed, as shown in Table 12.7.

Maximum Interface Speed	Default Path Cost
10 Gb/s	2,000
1 Gb/s	20,000
100 Mb/s	200,000
10 Mb/s	2,000,000

Table 12.7 *Default path costs based on interface speeds*

For example, an interface that has a maximum speed of 1000 Mb/s (1 Gb/s), but is currently running at a speed of 10 Mb/s, has a default path cost of **20,000**.

Link aggregation does not affect the default path cost. For example, if a trunk has four 1 Gb/s interfaces, the default path cost is **20,000**.

For MSTP, you can set two kinds of path costs, external and internal. For STP and RSTP, you can set an external path cost only.

- **External path cost**
  The **External Path Cost** setting is used to calculate the cost of sending spanning tree traffic through the interface to reach an adjacent spanning tree region. The spanning tree algorithm tries to minimize the total path cost between each point of the tree and the root bridge. The external path cost applies only to those interfaces (and trunks) that are members of instance **0**.
- **Internal path cost**
  The **Internal Path Cost** setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region. Note that the internal path cost applies only to bridges that support the MSTP mode. The internal path cost applies to those interfaces (and trunks) that are members of any instance, including instance **0**.

To summarize, STP and RSTP use external path costs only, and the costs apply to instance **0** interfaces only. MSTP uses both external and internal path costs, and the internal costs apply to interfaces in all spanning tree instances, including instance **0**.

13

Setting up a Redundant System

- Introducing redundant systems
- Configuring units of a redundant pair
- Specifying the default route on back-end servers
- Synchronizing configuration data
- Continuing with active-active system configuration
- Configuring fail-safe
- Mirroring connection information
- Setting a shared MAC masquerade address
- Maintaining a redundant system

Introducing redundant systems

A ***redundant system*** is a type of BIG-IP system configuration that allows traffic processing to continue in the event that a BIG-IP system becomes unavailable. A BIG-IP redundant system consists of two identically-configured BIG-IP units. When an event occurs that prevents one of the BIG-IP units from processing network traffic, the peer unit in the redundant system immediately begins processing that traffic, and users experience no interruption in service.

You can configure the units of a redundant system to run in one of two redundancy modes: active/standby or active-active.

- **Active/standby mode**
  With ***active/standby*** mode, only one of the two units is in an active state, that is, processing traffic, at any given time. The inactive unit serves strictly as a standby unit, becoming active only if the active unit becomes unavailable. When a standby unit becomes active, it normally remains active until an event occurs that requires the other unit to become active again, or until you specifically force it into a standby state. For more information, see *Understanding failover in active/standby mode*, on page 13-3, and *Configuring the redundancy mode*, on page 13-13.

- **Active-active mode**
  With ***active-active*** mode, both units are in an active state simultaneously, each processing traffic for different virtual servers or SNATs. If an event prevents one of the units from processing traffic, the other unit begins processing that traffic in addition to its own. When the failed unit becomes active again, it does not resume processing connections until you specifically direct it to do so. For more information, see *Understanding failover in active-active mode*, on page 13-4, and *Configuring the redundancy mode*, on page 13-13.

Summary of redundant system features

When you set up a redundant system, you configure a variety of features. Some of these features are required, while others are strictly optional. Table 13.1 shows the complete set of features that you can configure for a redundant system.

Feature	Description
Primary and secondary failover addresses	Not only can you specify the primary self IP addresses that a BIG-IP unit is to use for failover, but you can also specify a second pair of IP addresses, on a different VLAN. This secondary pair of IP addresses is for use in case the primary addresses are unavailable. Primary failover addresses are required, and secondary ones are optional.
Active/standby or active-active configuration	You can configure one unit of the redundant system to be active and the other to remain idle until failover occurs. Or, if you want to use both units of your redundant system to process connections simultaneously, you can configure an active-active system. This feature is required.
Redundancy state preference	You can set up one unit in a pair to be the dominant active BIG-IP system. The unit you set up as the dominant BIG-IP system always attempts to be active. This feature applies to active/standby systems only, and is optional.
Network-based failover	You can configure the BIG-IP system to use the network instead of a hard-wired connection to determine the status of the active unit. This feature is optional.
Configuration synchronization	With this feature, you can configure one BIG-IP unit and then synchronize the configuration with the other BIG-IP unit. This feature is required.
Global display of synchronization status	With this feature, you can display the current synchronization status of a unit on every screen of the Configuration utility. This feature is optional.
System fail-safe	With this feature, the BIG-IP system can monitor various hardware components and system services to detect failures. This feature is optional.
Gateway fail-safe	With this feature, the BIG-IP system can respond to the status of upstream routers. This feature is optional.
VLAN fail-safe	With this feature, a BIG-IP system can take action if a VLAN is no longer able to send or receive traffic. This feature is optional.
Connection mirroring	You can mirror connection and persistence information between redundant units. This enables you to provide seamless failover of client connections. This feature is optional.
Sharing a MAC masquerade address	You can share the media access control (MAC) masquerade address between BIG-IP units in a redundant system. This feature is useful if you want to use the system in a topology with secure hubs. This feature is optional.

Table 13.1 *Configurable features of a redundant system*

Understanding failover and failback

Perhaps the most important tasks that a redundant system performs are failover (to maintain availability when a specific BIG-IP system becomes unavailable), and failback (to re-establish normal BIG-IP system processing when a previously-unavailable BIG-IP system becomes available again).

What is failover?

Failover is a process that occurs when one system in a redundant system becomes unavailable, thereby requiring the peer unit to assume the processing of traffic originally targeted for the unavailable unit. To facilitate coordination of the failover process, each unit has a unit ID (1 or 2).

An essential element to making failover successful is a feature called configuration synchronization. Configuration synchronization, or ***ConfigSync***, is a process where you replicate one unit's main configuration file on the peer unit. Because data is shared in this way, a unit can process the other unit's traffic when failover occurs.

By default, the way that a BIG-IP unit monitors the status of its peer, in order to detect that failover is required, is through a hard-wired connection between the two BIG-IP units. With proper configuration, however, you can cause each BIG-IP unit to monitor peer status by way of a TCP/IP network connection instead. For more information on types of failover connections, see *Configuring the failover type*, on page 13-15.

Understanding failover in active/standby mode

When a redundant system is in active/standby mode, one unit is active, that is, accepting and processing connections on behalf of the redundant system, while the other unit is idle (that is, in a standby state).

When failover occurs, the standby unit becomes active, and it normally stays active until failover occurs again, or until you force it into a standby state. Forcing the unit into a standby state automatically causes the other system to become active.

For example, you can configure unit 1 to process traffic for virtual servers A and B. The standby unit monitors the active unit, and if communications fail, the standby unit initiates a failover and becomes the active unit. It then begins processing traffic for both virtual servers.

You can see an active/standby configuration, first as it behaves normally, and then after failover has occurred, by viewing Figure 13.1.

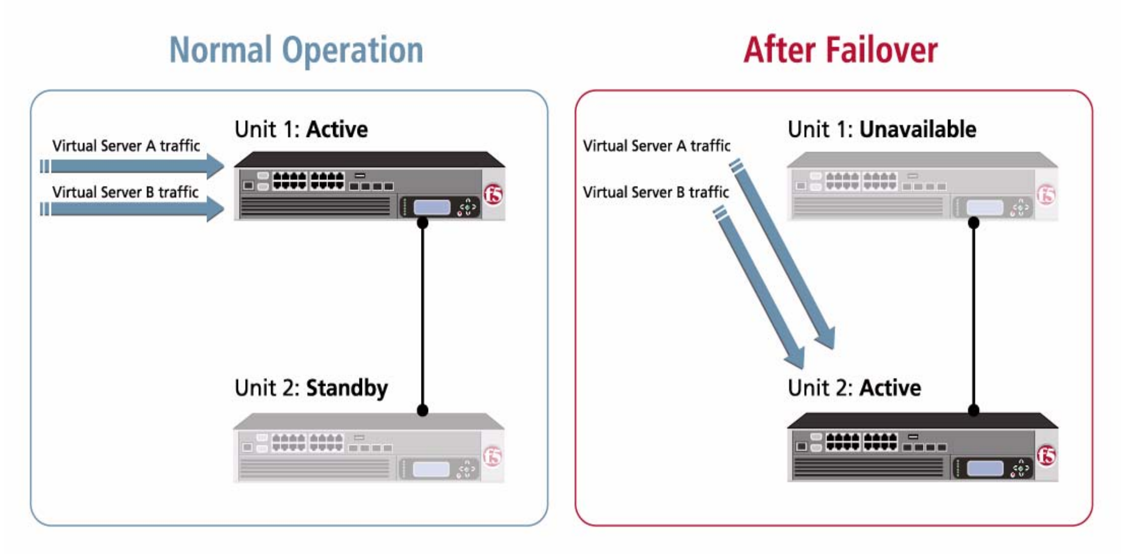


Figure 13.1 *Failover on an active/standby system*

As you can see in Figure 13.1, unit 1 is in an active state, and unit 2 is in a standby state. With this configuration, failover causes the following to occur:

- Unit 2 switches to an active state.
- Unit 2 begins processing the connections that would normally be processed by its peer.

When the failed unit becomes available again, you can force a unit to change its state from active to standby or from standby to active, thereby initiating failback. ***Failback*** on an active/standby system causes a unit to relinquish any processing that it is doing on behalf of its peer, and return to a standby state. A redundant system in active/standby mode is the most common type of redundant system. For more information on failback, see *What is failback?*, on page 13-6.

Understanding failover in active-active mode

Unlike an active/standby configuration, which is designed strictly to ensure no interruption of service in the event that a BIG-IP system becomes unavailable, an active-active configuration has an additional benefit. An active-active configuration allows the two units to simultaneously manage traffic, thereby improving overall performance.

A common active-active configuration is one in which each unit processes connections for different virtual servers. For example, you can configure unit 1 to process traffic for virtual servers A and B, and configure unit 2 to process traffic for virtual servers C and D. If unit 1 becomes unavailable, unit 2 begins processing traffic for all four virtual servers.

You can see an active-active configuration, first as it behaves normally, and then after failover has occurred, by viewing Figure 13.2.

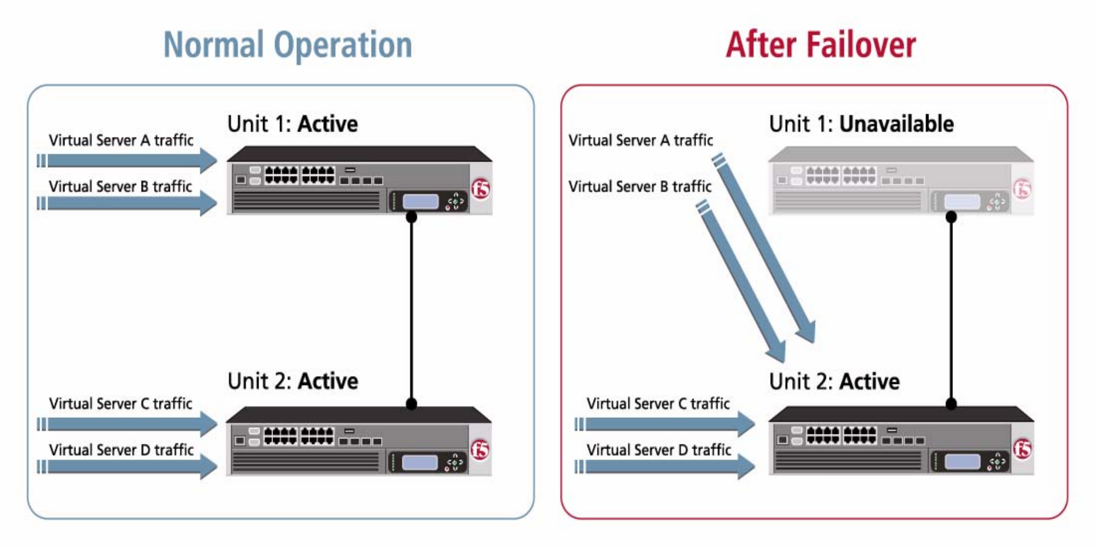


***Figure 13.2** Failover on an active-active system*

Figure 13.2 shows an active-active configuration in which units 1 and 2 are both in active states. With this configuration, failover causes the following to occur:

- Unit 2 (already in an active state) begins processing the connections that would normally be processed by unit 1.
- Unit 2 continues processing its own connections, in addition to those of unit 1.

When unit 1 becomes available again, you can initiate ***failback***, which, in this case, means that the currently-active unit relinquishes any processing that it is doing on behalf of its peer, and continues to operate in an active state, processing its own connections. From this point on, each unit in the active-active system handles its own unit-specific processing. For more information on failback, see *What is failback?*, following.

In addition to associating a unit in an active-active system with a specific virtual server, you can associate a unit with a particular SNAT. Thus, for an active-active configuration to operate successfully, you must associate each virtual server or SNAT with the unit of the redundant system that determines which active unit processes its connections.

What is failback?

Failback is the process of a previously unavailable unit reclaiming its normal traffic as soon as it returns to an active state. Failback behaves differently depending on the mode. For information on managing failback, see *Controlling failback*, on page 13-37.

Understanding self IP addresses for redundant systems

To successfully configure and maintain a redundant system, it is helpful to understand a redundant system's use of static and floating self IP addresses. Configured correctly, static and floating self IP addresses are a key aspect of ensuring that traffic processing continues uninterrupted when failover occurs.

Using static self IP addresses

A ***static self IP address*** is an IP address that you assign to a BIG-IP system's interface. During normal redundant-system operation prior to failover, the two units use the internal static self IP addresses to continually communicate with one another about system status.

You assign static self IP addresses to each unit's **internal** and **external** VLANs when you run the Setup utility on that unit. Then, when you use the Configuration utility to further configure each unit of your redundant system, you specify a pair of those static self IP addresses, known as a primary failover pair. The ***primary*** pair specifies the two internal static self IP addresses that the two units use to communicate with one another, before, during, and after failover. (These are the same static self IP addresses that you assigned when you ran the Setup utility on each unit.)

Optionally, you can specify a ***secondary*** pair, which specifies two alternate static self IP addresses to which failover should occur in the event that the primary addresses are unavailable. Note that the primary addresses typically reside on a different VLAN than the secondary addresses.

For more information on primary and secondary failover addresses, see *Specifying primary and secondary failover addresses*, on page 13-12.

Using floating self IP addresses

A ***floating self IP address*** is an IP address that is shared between two systems, or between two units of a redundant system. When you run the Setup utility, you normally assign a floating IP address to the internal interface of each unit (in addition to assigning a static self IP address).

Normally, for non-redudant systems (that is, single devices), it is the internal interface's static self IP address that appears as the source IP address in the header of a TCP packet going from a BIG-IP unit to a back-end server. This causes the back-end server to send its response to that static self IP address. If the BIG-IP system becomes unavailable, the system fails to receive the response.

With a redundant system, however, you can configure the back-end servers to send their responses to a shared floating IP address instead of a static self IP address, and if the target unit is unavailable, the peer unit can receive and process that traffic. Without this shared floating IP address, the delivery of back-end server traffic to the surviving BIG-IP unit would fail.

◆ **Important**

For an active/standby system, when you run Setup on each unit, you must assign the same internal floating IP address to each unit's internal interface. For an active-active system, you must assign a unique floating IP address to each unit's internal interface.

It is sufficient for units of an active/standby configuration to share the same internal floating IP address, but it is not sufficient for an active-active configuration, for these reasons:

- For an active/standby configuration, sharing one internal floating IP address between the two units is sufficient because in the event of failover, the failover unit can always use this address to receive and process all of the unavailable unit's incoming back-end server traffic.
- For an active-active configuration, each unit needs its own internal floating IP address, which the unit shares with its peer (using ConfigSync). Then, based on which of the two floating IP addresses a given back-end server uses to send its responses, the surviving unit can correlate the response to the correct unit's virtual servers and SNATs, and process the response accordingly. For information on configuring back-end servers to use floating IP addresses, see *Specifying the default route on back-end servers*, on page 13-16.

Example of using a floating IP address for an active/standby system

For an active/standby system, suppose that when you initially ran the Setup utility on unit 1, you specified **11.12.11.3** as the internal floating IP address, and when you ran Setup on unit 2, you also specified **11.12.11.3** as its internal floating IP address. When you synchronize the configurations later, **11.12.11.3** should appear on both units as the floating IP address belonging to unit 1.

Then, if unit 1 fails over:

- Unit 2 assumes the unit 1 internal floating IP address (**11.12.11.3**).
- The back-end servers that normally send traffic to the internal address **11.12.11.3** on unit 1 continue to send their traffic to that same address, even though this incoming traffic is now processed by unit 2.
- Unless configured otherwise, unit 2 continues processing traffic until failover occurs again.

Example of using floating IP addresses for an active-active system

For an active-active system, suppose that when you initially ran the Setup utility on unit 1, you specified **11.12.11.3** as the internal floating IP address, and when you ran Setup on unit 2, you specified **11.12.11.4** as its internal floating IP address. When you synchronize the configurations later, **11.12.11.3** should appear on both units as the floating IP address belonging to unit 1, and **11.12.11.4** should appear on both units as the floating IP addresses belonging to unit 2.

Then, if unit 1 fails over:

- Unit 2 assumes the internal floating IP address of unit 1 (**11.12.11.3**).
- The back-end servers that normally send traffic to the internal address **11.12.11.3** on unit 1 continue to send their traffic to that same address, even though this incoming traffic is now processed by unit 2.
- The back-end servers that normally send traffic to the internal address **11.12.11.4** on unit 2 continue to send their traffic to that same address.

Conversely, if unit 2 fails over:

- Unit 1 assumes the internal floating IP address of unit 2 (**11.12.11.4**).
- The back-end servers that normally send traffic to the internal address **11.12.11.4** on unit 2 continue to send their traffic to that same address, even though this incoming traffic is now processed by unit 1.
- The back-end servers that normally send traffic to the internal address **11.12.11.3** on unit 1 continue to send their traffic to that same address.

◆ **Tip**

You can configure additional floating IP addresses on the external VLANs of each BIG-IP system as well. This makes it possible for routers to route to a virtual server using virtual ***noarp*** *mode.*

Understanding fail-safe

Fail-safe is the ability of a unit in a redundant system configuration to monitor certain aspects of the system or network, detect interruptions, and consequently take some action, such as initiating failover to the peer unit. Fail-safe can apply to system services, traffic between the BIG-IP system and a gateway router, or VLAN traffic. For more information, see *Configuring fail-safe*, on page 13-24.

Before you begin

Before you begin using this chapter to set up a redundant system, you must run the Setup utility on each unit that is to make up the redundant system if you have not already done so. When you run the Setup utility on a BIG-IP system, you provide some essential information:

- A designation that the system is either a single device or part of a redundant pair
- Static self IP addresses for the VLANs
- Floating self IP addresses for the VLANs

Once you have supplied this information, you can use the remainder of this chapter to complete the configuration of your redundant system. You must first decide, however, whether you want your redundant system to operate in active/standby mode or active-active mode. Then you can use the Configuration utility to configure the two units of your redundant system accordingly. You also need to perform one other configuration task on the back-end servers to which the redundant system sends network traffic.

The remainder of this chapter describes in detail all of the tasks that you must perform to set up a redundant system. In summary, you must:

- Configure individual settings on each BIG-IP unit, such as redundancy mode and failover IP addresses. For more information, see *Configuring units of a redundant pair*, on page 13-11.
- Configure the default route on each back-end server. For more information, see *Specifying the default route on back-end servers*, on page 13-16.
- Synchronize the configuration data from unit 1 to unit 2. For more information, see *Synchronizing configuration data*, on page 13-18.
- If using active-active mode, associate each virtual server, self IP address, and SNAT with a unit ID, and synchronize the configuration data from unit 2 to unit 1. For more information, see *Continuing with active-active system configuration*, on page 13-22.
- Configure fail-safe settings for system hardware and services, gateway router traffic, and VLAN traffic. For more information, see *Configuring fail-safe*, on page 13-24.

You can also perform two optional tasks:

- ◆ Mirror connection information. For more information, see *Mirroring connection information*, on page 13-29.
- ◆ Set a shared MAC masquerade address. For more information, see *Setting a shared MAC masquerade address*, on page 13-30.

Once your redundant system is operational, the BIG-IP system displays an indicator in the upper-left corner of all Configuration utility screens, to indicate this information:

- The unit you are currently managing (unit 1 or unit 2)
- The current state of the unit (active or standby)
- Configuration synchronization status (this display is optional)

◆ **Note**

*For information on how to manage a unit of a redundant system on an ongoing basis, see **Maintaining a redundant system**, on page 13-33.*

Configuring units of a redundant pair

To configure a redundant system, you must first configure certain settings on each unit that is to be part of the redundant pair, using the Configuration utility. For some settings, you can simply use a default value.

The settings that you must configure are:

- Primary and secondary failover addresses for a unit and its peer
- The redundancy mode (active/standby or active-active)
- For an active/standby system, the preferred redundancy state for a unit (none, active, or standby)
- The failover method (hard-wired or network)
- The link down time after a failure

Before you configure these settings on a unit, however, you should ensure that the unit is already designated as being part of a redundant pair. (You typically designate a unit as being part of a redundant pair when you initially run the Setup utility on that unit.)

To ensure redundant-system designation for a unit

1. On the Main tab of the navigation pane, expand **System**, and click **Platform**.
   The General screen opens.
2. In the General Properties area, verify that the **High Availability** list is set to **Redundant Pair**. If not, select this value.
3. For the **Unit ID** list, retain or change the value, depending on which unit ID you want to assign to this BIG-IP system.
4. Click **Update**.

After verifying the unit’s redundant-system designation, use the Configuration utility to perform the following procedure on each unit. When performed on each unit, this procedure creates either an active/standby or an active-active system. Note that the steps in this procedure provide only basic configuration information; the pages following the procedure provide more detailed information for each step, to help you configure the settings in a way that best suits your needs.

◆ **Important**

*The default type of redundant system that you create using this procedure is an active/standby system. For active-active configurations, you must perform additional configuration tasks after using the Configuration utility. For detailed information, see **Continuing with active-active system configuration**, on page 13-22.*

To configure a redundant system

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. For the **Primary Failover Address** boxes, in the **Self** box type the primary static self IP address for the unit that you are currently configuring, and in the **Peer** box type the primary static self IP address for the peer unit. For more information, see *Specifying primary and secondary failover addresses*, on page 13-12.

   ***Note**: Before typing the IP addresses, delete the two colons (::) in each box.*
3. If you want to configure the **Secondary Failover Address** settings, in the **Self** box type the secondary static self IP address for the unit you are currently configuring, and in the **Peer** box type the secondary static self IP address for the peer unit. For more information, see *Specifying primary and secondary failover addresses*, on page 13-12.

   ***Note**: Before typing the IP addresses, delete the two colons (::) in each box.*
4. From the **Redundancy Mode** list, either retain the default value of **Active/Standby**, or select **Active/Active**. For more information, see *Configuring the redundancy mode*, on page 13-13.
5. From the **Redundancy State Preference** list, select a preferred state for the unit you are configuring. For more information, see *Specifying a redundancy state preference*, on page 13-14.
6. If you want the system to use the network type of failover rather than hard-wired failover, check the **Network Failover** box. For more information, see *Configuring the failover type*, on page 13-15.
7. If you want an interface down time other than **0.0**, type a value in the **Link Down Time on Failover** box. For more information, see *Specifying the link down-time on failover*, on page 13-15.
8. Click **Update**.

Specifying primary and secondary failover addresses

When you configure a redundant system with the Configuration utility, you typically specify the internal static self IP addresses of the two peer systems in the redundant configuration. Each IP address that you specify for a unit is the static self IP address that you previously assigned to the unit’s internal interface when you ran the Setup utility on that unit.

Known as the ***primary failover addresses***, these are the IP addresses that the two BIG-IP units use to communicate with each other before, during, and after failover.

You use the **Self** setting to specify the internal static self IP address of the unit you are currently configuring as part of the redundant system. You use the **Peer** setting to specify the internal static self IP address of the other unit that you want to configure as part of the redundant system.

◆ **Tip**

*For background information on static self IP addresses, see **Using static self IP addresses**, on page 13-6.*

For example, suppose you want to configure an active/standby system in which the active unit has an internal static self IP address of **10.10.10.1** (unit 1) and the standby unit has an internal static self IP address of **10.10.10.2** (unit 2):

- On unit 1, you set the **Self** and **Peer** addresses in the **Primary Failover Addresses** setting to **10.10.10.1** and **10.10.10.2**, respectively.
- On unit 2, you set the **Self** and **Peer** addresses in the **Primary Failover Addresses** setting to **10.10.10.2** and **10.10.10.1**, respectively.

Optionally, you can specify ***secondary failover addresses***, which are static self IP addresses that the BIG-IP system uses if the primary failover addresses are unavailable for some reason.

◆ **Note**

Secondary failover addresses cannot reside on the same VLAN as primary failover addresses.

◆ **Important**

*For the **Primary Failover Address** and **Secondary Failover Address** settings, check that you have removed the two colons (**::**) from these boxes. Failure to do so could cause problems when you synchronize the configuration of the two units.*

Configuring the redundancy mode

Configuring the redundancy mode means specifying whether your redundant system runs in active/standby mode or active-active mode. If you choose active/standby mode, you can specify whether you prefer that unit to be an active or a standby unit when both units are available for processing traffic. For information on setting a preference for a unit's redundancy state, see *Specifying a redundancy state preference*, on page 13-14.

◆ **WARNING**

MAC masquerading is not supported in active-active mode.

For more information on active/standby and active-active configurations, see *Understanding failover and failback*, on page 13-2. For more information on MAC masquerading, see *Setting a shared MAC masquerade address*, on page 13-30.

Specifying a redundancy state preference

When you configure a system to be part of an active/standby redundant system, you can specify whether you want that system to function primarily as the active system or the standby system in the event that both units can be active at the same time. You can also can specify that you have no preference.

The preferences you can set are:

- **None**
  Specifies that this unit does not have a preferred redundancy state.
  In this case, failback does not normally occur, because a standby unit that becomes active due to failover remains active until failover occurs again. However, you can actively initiate failback when the unavailable unit becomes available again, by forcing the currently-active unit to revert to a standby state.

- **Active**
  Specifies that this unit is the preferred active unit. If you choose this option, the unit can be in a standby state due to a failover event. However, failback to this unit is automatic when this unit becomes available.

- **Standby**
  Specifies that this unit is the preferred standby unit. If you choose this option, then the unit can be in an active state due to a failover condition. However, failback to the peer unit is automatic when the peer unit becomes available.

A redundant system unit that prefers to be active can still serve as the standby unit when the redundant system already has an active unit. For example, if an active unit that prefers to be active fails over and is taken out of service for repair, it can then go back into service as the standby unit until the next time that the redundant system needs an active unit, for example, at reboot.

Configuring the failover type

To enable a unit to fail over to its peer system, you must first specify the type of failover that you want the redundant system to use. The two possible failover types are hard-wired failover and network-based failover.

- **Hard-wired failover**
  When you configure ***hard-wired*** failover, you enable failover by using a failover cable to physically connect the two redundant units. This is the default setting. For the procedure on configuring hard-wired failover, see ***Platform Guide: 1500, 3400, 6400, and 6800***.
- **Network failover**
  When you configure ***network*** failover, you enable failover by configuring your redundant system to use the network to determine the status of the active unit. You can use network failover in addition to, or instead of, hard-wired failover.

For background information on failover, see *Understanding failover and failback*, on page 13-2.

Specifying the link down-time on failover

When configuring a unit of a redundant system configuration, you can use the **Link Down Time on Failover** setting to specify the amount of time, in seconds, that interfaces for any external VLANs are down when the unit fails over and goes to a standby state. Specifying a value other than **0** for this setting causes other vendor switches to use the specified time to learn the MAC address of the newly-active unit.

The allowed value for this setting is **0** to **60**. Setting the value to **0** disables this setting.

Specifying the default route on back-end servers

Once you have used the Redundancy Properties screen of the Configuration utility to configure various settings on each unit, you can perform the next task, configuring the default route on each back-end server. (For a high-level summary of tasks, see *Before you begin*, on page 13-8.)

◆ **Tip**

For any back-end server that receives requests from a unit of a redundant system, you do not need to perform this step if the relevant virtual server is associated with a SNAT.

When failover occurs on a BIG-IP system, the surviving BIG-IP unit begins handling the inbound virtual-server connections (those targeted to back-end servers) that are normally processed by the failed unit, and begins handling the outbound connections (those originating from back-end servers) that are normally destined for the failed BIG-IP unit.

For a redundant system to do this properly, you need to set the default route for each back-end server to the shared, floating IP address assigned to the BIG-IP unit that normally processes the server's responses. This ensures that the back-end server can successfully send a response to the surviving BIG-IP unit.

For example, for an active/standby configuration, if the server **http_server** normally receives connections from unit 1 of your redundant system, and the floating IP address shared by the two units is **11.12.11.3**, you must set the default route for server **http_server** to **11.12.11.3**. Then, if unit 1 goes out of service, the surviving unit (unit 2) can receive the server's response because the IP address **11.12.11.3** is a shared IP address.

◆ **Note**

Follow your server vendor's instructions for the procedure on setting a default route.

Special considerations for active-active systems

When the surviving unit takes over a virtual server of the failed unit (in addition to having its own virtual servers), the surviving unit must know which virtual server to use to process traffic that it receives from a back-end server. The way it knows this is by the floating IP address to which the response was sent. (As described previously, in an active-active configuration, each unit must have its own unique floating IP address.)

For example, suppose the following:

- The floating IP address of unit 1 is **11.12.11.3**, and the floating IP address of unit 2 is **11.12.11.4**.

- Server **http_server** normally handles traffic for unit 1, which has virtual server **vs_http**. Server **smtp_server** normally handles traffic for unit 2, which has virtual server **vs_smtp**.
- You have configured the default routes of the servers accordingly. That is, you have set the default route of **http_server** to **11.12.11.3**, and the default route of **smtp_server** to **11.12.11.4**.

If unit 1 fails, the surviving unit (unit 2) now has both virtual servers (**vs_http** and **vs_smtp**).

Continuing with our previous example of back-end server **http_server**, if the surviving unit receives a response from **http_server** (sent to **11.12.11.3**, the unit 1 floating IP address), the surviving unit knows, based on that IP address, that the traffic is to be processed by the unit 1 virtual server **vs_http** (now on unit 2).

Similarly, if the surviving unit receives a response from server **smtp_server** (sent to **11.12.11.4**, the unit 2 floating IP address), the surviving unit knows, based on that IP address, that the traffic is to be processed by its own virtual server, **vs_smtp**.

Thus, if you have 20 servers and half of them normally serve the unit 1 virtual servers, you must configure the default route for those 10 servers to be the floating IP address of unit 1. For the remaining 10 servers in your network, which serve the unit 2 virtual servers, you must configure their default route to be the floating IP address of unit 2.

By setting the default routes of your back-end servers to the floating IP address of either unit 1 or unit 2, you ensure that if a unit becomes unavailable, any connections that the servers normally send to that unit are received and processed by the surviving unit, because the surviving unit has assumed the internal floating IP address of the failed machine.

◆ **Tip**

*For information on initially assigning floating IP addresses to redundant-system units, see **Using floating self IP addresses**, on page 13-6.*

The next step

When you have completed the procedure for configuring a redundant system, you need to synchronize the configuration data. To do this, proceed to *Synchronizing configuration data*, on page 13-18.

Note that if you are setting up an active-active system, you must perform additional configuration tasks after performing synchronization. For more information, see *Continuing with active-active system configuration*, on page 13-22.

Synchronizing configuration data

Once you have completed the initial configuration of one of the units in your redundant system, you must synchronize the configuration between the two units. For an active/standby system, you must perform configuration synchronization from the active unit to the standby unit. For an active-active system, you must perform synchronization from each unit to the other.

When you synchronize data from one unit to another, you are giving the target unit the data that it needs to assume traffic processing for its peer when failover occurs. Examples of configuration data that a target unit receives during configuration synchronization are virtual servers, SNATs, and floating IP addresses.

◆ **Important**

If you plan to run your redundant system in active-active mode, you must perform other configuration tasks after you have initially synchronized the configuration data from one unit to another. After performing those additional tasks, you must then synchronize the configuration data again. For more information, see ***Continuing with active-active system configuration****, on page 13-22.*

You can synchronize configuration data from the current system to the peer system, or you can synchronize the data from the peer system to the current system. The method you choose depends on which unit's data has most recently changed and which unit you are currently configuring.

When you perform configuration synchronization, the BIG-IP system copies a **.ucs** file containing configuration data from one unit to the other. You must synchronize the configuration data before you can put any redundant system into operation.

◆ **Note**

Prior to synchronizing configuration data, the BIG-IP system creates a backup configuration file on the target system, as a preventative measure.

With respect to configuration synchronization, you can use the Configuration utility to:

- Perform configuration synchronization
- Enable the global display of synchronization status
- View peer synchronization status (for more information, see *Viewing synchronization status*, on page 13-34)

Performing configuration synchronization

When you have a redundant system configuration, it is essential that each unit shares, or ***synchronizes***, its current configuration data with its peer unit. If a unit does not share its configuration data with its peer, the surviving unit cannot process traffic for that peer unit. For this reason, you must synchronize configuration data when you initially configure the redundant system, and then repeatedly, on an ongoing basis. The need to repeatedly synchronize data is because a unit's configuration data typically changes over time during normal system maintenance, such as when you add a virtual server or create a new profile, and the unit must share those changes with its peer.

◆ **Tip**

*You can easily determine when to synchronize configuration data by using the Configuration utility to view synchronization status. Synchronization status indicates whether the configuration data of the units is synchronized. For more information, see **Viewing synchronization status**, on page 13-34.*

You synchronize configuration data using the ConfigSync screen that is available from the Redundant Properties screen of the Configuration utility. The ConfigSync screen contains two settings that are directly related to performing configuration synchronization between redundant units: **ConfigSync User** and **Synchronize**.

To synchronize configuration data

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. On the menu bar, click **ConfigSync**.
   The ConfigSync screen opens.
3. If the user name you are using is other than **admin**:

   a) Find the **Configuration** heading and select **Advanced**.

   b) For the **ConfigSync User** setting, select a user name from the **Name** list.
   This displays the **Password** box.

   c) In the **Password** box, type the password for the selected user name.

   ***Note:** For more information, see **Specifying the ConfigSync user**, on page 13-20.*
4. If you want to encrypt the configuration data, then from the **Encryption** box, select **On**.

   ***Note:** If you want encrypted configuration data to be included in archive files, use the Preferences screen to turn on the **Archive Encryption** setting.*

5. If you want the BIG-IP system to display synchronization status on every screen of the Configuration utility, locate the **Detect ConfigSync Status** setting and check the **Enabled** box.
   For more information, see *Enabling the global display of synchronization status*, on page 13-21.
6. For the **Synchronize** setting, click **Synchronize TO Peer** or **Synchronize FROM Peer**.
   For more information, see *Specifying synchronization direction*, on page 13-20.
7. Click **Update**.

Specifying the ConfigSync user

The **ConfigSync User** setting allows you to specify the name of the user who is allowed to perform configuration synchronization. In order for configuration synchronization to function correctly, the name and password for the **ConfigSync User** account must be the same on both BIG-IP units. Whenever you change the **ConfigSync User** password, the BIG-IP system reminds you to update the password on the peer unit.

Only users with the **Adminstrator** role assigned to their user accounts can perform configuration synchronization. Consequently, all existing BIG-IP system user accounts that have the **Administrator** role assigned to them appear in the **Name** list.

The default user account name for the **ConfigSync User** setting is **admin**. If you want to perform a configuration synchronization and you are not user **admin,** you must select a user name from the **Name** list and type your password.

If you want to give a user other than yourself permission to perform a configuration synchronization, and the user name does not appear in the **Name** list, use the Users screen to assign the **Administrator** role to that user account.

◆ **Note**

You do not need to type the password for the ***admin*** *account.*

Specifying synchronization direction

The **Synchronize** setting allows you to perform a configuration synchronization between two units. To synchronize data, you can click either of the following buttons:

- **Synchronize TO Peer**
  Use this button when the unit you are currently configuring contains updated configuration data that you want to share with the peer unit.

- **Synchronize FROM Peer**
  Use this button when the peer unit contains updated configuration data that you want to share with the unit you are currently configuring.

In either case, the term ***peer*** refers to the unit with the self IP address that appears in the **ConfigSync Peer** box.

Enabling the global display of synchronization status

To ensure that you are aware of any need to synchronize configuration data, you can display synchronization status on each screen of the Configuration utility. You enable this display of synchronization status on the ConfigSync screen, using the **Detect ConfigSync Status** setting. If you check this box, the BIG-IP system displays, on every screen of the Configuration utility, the current synchronization status of the unit you are configuring.

◆ **Tip**

*The Configuration utility also displays more detailed synchronization status information. For complete information on viewing configuration synchronization status, see **Viewing synchronization status**, on page 13-34.*

Continuing with active-active system configuration

To fully configure an active-active redundant system, you must perform other tasks in addition to those described in *Before you begin*, on page 13-8. These tasks are:

- Associating the virtual servers and SNATs with the relevant unit number. You perform this task on both units.
- Synchronizing the configuration to the peer unit. You perform this task on both units.

You use the **bigpipe** command-line utility to perform the first task. You use the Configuration utility to perform the second task, synchronizing the configuration.

Associating BIG-IP system objects with unit IDs

Each BIG-IP system in an active-active configuration has a unit ID, either **1** or **2**. When you define a local traffic management object, such as a virtual server, you must associate that object with a specific unit of the active-active redundant pair. When failover occurs, these associations of objects to unit IDs allow the surviving unit to process connections correctly for itself and the failed unit.

You must associate these local traffic management objects with a unit ID:

- Virtual servers
- Self IP addresses
- SNATs

For example, associating virtual server A with unit 1 causes unit 1 to process connections for virtual server A. Associating virtual server B with unit 2 causes unit 2 to process connections for virtual server B. This allows the two units to process traffic for different virtual servers simultaneously, and results in an increase in overall performance. If one of the units fails over, the remaining unit begins processing the connections for all virtual servers of the redundant pair, until failback occurs.

This scenario of using the two units to process different connections simultaneously is one reason for the requirement that both units store identical configuration files (**/config/bigip.conf**).

If you do not associate an object with a specific unit ID in an active-active redundant pair, the redundant system uses **1** as the default unit ID.

Associating a virtual server with a unit ID

You can view a list of virtual servers and their associated unit IDs, and you can change the unit ID associated with a specific virtual server. You can perform these tasks using the **bigpipe** command-line utility.

To view an existing virtual server-unit ID association

To view the unit ID associated with your existing virtual servers, use this **bigpipe** command syntax:

```
b virtual address [<ip addr list> | all] unit [show]
```

To change the unit ID associated with a virtual server

To change the unit ID associated with an existing virtual server, type this command sequence:

```
b virtual address <ip addr> unit <id>
```

Associating a self IP address with a unit ID

You can view a list of self IP addresses and their associated unit IDs, and you can change the unit ID associated with a specific self IP address.

To view an existing self IP address-unit ID association

To view the unit ID associated with your existing self IP addresses, use this **bigpipe** command syntax:

```
b self [<ip addr list> | all] unit [show]
```

To change the unit ID associated with a self IP address

To change the unit ID associated with an existing self IP address, type this command sequence:

```
b self <ip addr> unit <id>
```

Associating a SNAT with a unit ID

You can view a list of SNATS and their associated unit IDs, and you can change the unit ID associated with a specific SNAT. You can perform these tasks using the **bigpipe** command-line utility.

◆ **Note**

You cannot associate a default SNAT with a unit ID. The default SNAT is not compatible with an active-active system.

To view an existing SNAT-unit ID association

To view the unit ID associated with your existing SNAT translation addresses, use this **bigpipe** command syntax:

```
b snat translation [<ip addr list> | all] unit [show]
```

To change the unit ID associated with a SNAT address

To change the unit ID associated with an existing SNAT translation address, type this command sequence:

```
b snat translation <ip addr> unit <id>
```

Synchronizing the configuration

When you used the Redundancy Properties screen to initially configure each unit of the active-active system, you also synchronized the configurations between the two units. Now that you have associated unit IDs with each virtual server, self IP address, and SNAT, you must synchronize the configurations again. For more information, see *Synchronizing configuration data*, on page 13-18.

Configuring fail-safe

Fail-safe is the ability of a BIG-IP system to monitor certain aspects of the system or network, detect interruptions, and consequently take some action. In the case of a redundant system, a unit can detect a problem and initiate failover to the peer unit. When you configure the fail-safe feature on a BIG-IP system, you are specifying the particular events that cause failover to occur in a redundant system. The fail-safe feature applies to:

- System services
- Traffic between the BIG-IP system and a gateway router
- Traffic on a VLAN

Configuring system fail-safe

When you configure system fail-safe, the BIG-IP system monitors various hardware components, as well as the heartbeat of various system services, and takes action if the system detects a failure.

Configuring hardware-component monitoring

You can configure the BIG-IP system to monitor the switch board component and then take some action if the BIG-IP system detects a failure.

Using the Configuration utility, you can specify the action that you want the BIG-IP system to take when the component fails. Possible actions that the BIG-IP system can take are:

- Reboot the BIG-IP system.
- Restart all system services.
- Fail over to the peer system.
- Fail over and abort the TMM service.
- Take no action.

To configure hardware-component monitoring

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. From the Fail-safe menu, choose System.
   The System Fail-safe screen opens.
3. In the System Trigger Properties area, for **Hardware Monitor**, verify that the box is checked.
4. From the **Switch Board Failure** list, select an action, or retain the default setting (**Fail Over and Abort TMM**).
5. Click **Update**.

Configuring system-service monitoring

You can configure the BIG-IP system to monitor various system services and then take some action if the BIG-IP system detects a heartbeat failure. These services are:

- MCPD (messaging and configuration)
- TMM (traffic management)
- BIGD (health monitors)
- SOD (failover)
- BCM56XXD (switch hardware driver)

Using the Configuration utility, you can specify the action that you want the BIG-IP system to take when the heartbeat of a system service fails. Table 13.2 lists each system service, and shows the possible actions that the BIG-IP system can take in the event of a heartbeat failure.

System Service	Possible actions
MCPD	Restart the system service. Restart all system services. Reboot the BIG-IP system. Fail over to the peer system. Fail over to the peer system and restart the service. Take no action.
TMM	
BIGD	
SOD	Reboot the system. Restart all system services. Take no action.
BCM56XXD	Restart the system service. Take no action.

Table 13.2 *Possible actions in response to heartbeat failure*

To configure system-service monitoring

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. From the Fail-safe menu, choose System.
   The System Fail-safe screen opens.
3. In the System Services area, in the Name column, click the name of the service you want to monitor.
   The screen for that service opens.
4. From the **Heartbeat Failure** list, select an action, or retain the default setting.
5. Click **Finished**.
   The System Fail-safe screen opens.
6. Click **Update**.

For more information on system services, see Chapter 18, *Configuring BIG-IP System Services*.

Configuring gateway fail-safe

Fail-safe features on the BIG-IP system provide network failure detection based on network traffic. One type of network failure detection is known as gateway fail-safe. ***Gateway fail-safe*** monitors traffic between the active BIG-IP system and a pool containing a gateway router, thereby protecting the system from a loss of an internet connection by triggering a failover when a gateway router is unreachable for a specified duration. If you want failover to occur when a gateway router is unreachable, you can configure the gateway fail-safe feature.

You can configure gateway fail-safe using the Configuration utility. Configuring gateway fail-safe means designating a load balancing pool as a gateway fail-safe pool.

When you designate a pool as a gateway fail-safe pool, you provide the following information:

- Name of the pool
- The unit ID number of the peer on which the gateway pool is configured
- The minimum number of gateway pool members that must be available to avoid the designated action
- The action that the BIG-IP system should take when the number of available gateway pool members drops below the designated threshold. Possible actions are **Reboot**, **Fail Over**, and **Restart All**. The default value is **Fail Over**.

To configure gateway fail-safe

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. From the Fail-safe menu, choose Gateway.
   The Gateway Fail-safe screen opens.
3. In the upper-right corner of the screen, click **Add**.
   The Add Gateway Pool screen. opens.
4. From the **Gateway Pool** list, select the name of a load balancing pool.
5. From the **Unit ID** list, select a unit ID for the pool (**1** or **2**).
6. In the **Threshold** box, type the number of pool members that must be available to avoid the action designated in the **Action** setting.
7. From the **Action** list, select an action (**Reboot**, **Fail Over**, or **Restart All**).
8. Click **Finished.**

Configuring VLAN fail-safe

For maximum reliability, the BIG-IP system supports failure detection on all VLANs. When you configure the fail-safe option on a VLAN, the BIG-IP system monitors network traffic going through a VLAN. If the BIG-IP system detects a loss of traffic on a VLAN and the fail-safe timeout period has elapsed, the BIG-IP system attempts to generate traffic by issuing ARP requests to nodes accessible through the VLAN. The BIG-IP system also generates an ARP request for the default route, if the default router is accessible from the VLAN. Failover is averted if the BIG-IP system is able to send and receive any traffic on the VLAN, including a response to its ARP request.

If the BIG-IP system does not receive traffic on the VLAN before the timeout period expires, it can either initiate failover and switch control to the standby unit, reboot, or restart all system services. The default action is **Restart All.**

◆ **WARNING**

You should configure the fail-safe option on a VLAN only after the BIG-IP system is in a stable production environment. Otherwise, routine network changes might cause failover unnecessarily.

Each interface card installed on the BIG-IP system is typically mapped to a different VLAN. Thus, when you set the fail-safe option on a particular VLAN, you need to know the interface to which the VLAN is mapped. You can use the Configuration utility to view VLAN names and their associated interfaces.

There are two ways to configure VLAN fail-safe: from the Redundancy Properties screen, or from the VLANs screen.

To configure VLAN fail-safe using the Redundancy Properties screen

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. From the Fail-safe menu, choose VLANs.
   The VLAN Fail-safe screen opens.
3. In the upper-right corner of the screen, click **Add**.
   The Add VLAN screen opens.
4. From the **VLAN** list, select a VLAN name.
5. In the **Timeout** box, specify the period of time during which traffic should be detected on the VLAN, after which the designated action will occur.
   The default value, in seconds, is **30**.
6. From the **Action** list, select the action that the BIG-IP system should take when the timeout period expires.
   Possible actions are **Reboot**, **Fail Over**, and **Restart Al**l.
7. Click **Finished**.

To configure VLAN fail-safe using the VLANs screen

1. On the Main tab of the navigation screen, expand **Network**, and click **VLANs**.
   This opens a list of existing VLANs.
2. Click the name of an existing VLAN, or click **Create**.
3. For the **Configuration** heading, select **Advanced**.
4. In the **Fail-safe** setting, check the box.
   This shows additional settings.
5. In the **Fail-safe Timeout** box, specify the period of time during which traffic should be detected on the VLAN, after which the designated action will occur.
   The default value, in seconds, is **30**.
6. From the **Action** list, select the action that the BIG-IP system should take when the timeout period expires.
   Possible actions are **Reboot**, **Fail Over**, and **Restart Al**l.
7. Click **Update** or **Finished**.

Mirroring connection information

The failover process of a redundant system ensures that a BIG-IP system is always available to process connections with no discernible interruption in service at the time of the failure event. However, failover does not preserve the specific connections on your servers at the moment of failover; connections are dropped when an active unit becomes unavailable, unless you have enabled connection mirroring.

The ***connection mirroring*** feature on the BIG-IP system duplicates a unit's state (that is, real-time connection and persistence information) on the peer unit. When connection mirroring is enabled, failover can be so seamless that file transfers can proceed uninterrupted and your servers can generally continue with whatever they were doing at the time of failover.

◆ **Note**

You cannot mirror Secure Sockets Layer (SSL) connections.

To enable connection mirroring for a virtual server

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **Virtual Servers**.
   This opens the Virtual Servers screen, which displays a list of existing virtual servers.
2. Click the name of a virtual server.
   This shows the properties for that virtual server.
3. Next to the Configuration heading, select **Advanced**.
4. Scroll down to the **Connection Mirroring** setting and check the box.
5. Click **Update**.

To enable connection mirroring for a SNAT

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **SNATs**.
   This opens the SNATs screen, which displays a list of existing SNATs.
2. Click the name of a SNAT.
   This displays the properties for that SNAT.
3. In the Configuration area, locate the **Stateful Failover Mirror** setting and check the box.
4. Click **Update**.

In addition to setting up connection mirroring, you can change the values of several bigdb database keys related to mirroring. For more information, see the man page for the **bigpipe db** command.

Setting a shared MAC masquerade address

For active/standby systems only, you can share the media access control (MAC) masquerade address between BIG-IP units. This feature is useful if you want to use the system in a topology with secure hubs. Sharing the MAC masquerade address between units has the following advantages:

- Increased reliability and failover speed, especially in lossy networks
- Interoperability with switches that are slow to respond to the network changes
- Interoperability with switches that are configured to ignore network changes

A BIG-IP unit uses the shared MAC address when it is the active unit in a redundant system. When the unit is in a standby state, the system uses the actual MAC address of the interface. Note that this option is valid only for active/standby mode.

◆ **Note**

For sensible operation, you must set the MAC masquerade address to be the same on both the active and standby units.

Viewing interfaces and MAC addresses

The MAC address for a VLAN is the MAC address of the first interface to be mapped to the VLAN, typically 4.1 for external and 5.1 for internal. You can view the interfaces mapped to a VLAN using the Configuration utility.

To view the interfaces mapped to a VLAN

1. On the Main tab of the navigation pane, expand **Network**, and click **VLANs**.
   This opens the VLANs screen, which displays a list of existing VLANs.
2. In the Untagged Interfaces or Tagged Interfaces column, view the interfaces mapped to each VLAN.

You can also view the MAC addresses for the interfaces on the BIG-IP system.

To view the MAC address for an interface

1. On the Main tab of the navigation pane, expand **Network**, and click **Interfaces**.
   This opens the Interfaces screen, which displays a list of existing interfaces.
2. In the MAC Address column, view the MAC address for each interface.

Designating a shared MAC masquerade address

The first step in designating a MAC masquerade address that the redundant units can share is to find the MAC address on both the active and standby units, and choose an address that is similar but unique. A safe technique for selecting the shared MAC address follows.

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

```
Active: 3.1 = 0:0:0:ac:4c:a2
Standby: 3.1 = 0:0:0:ad:4d:f3
```

To avoid packet collisions, you now must choose a unique MAC 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** is a suitable shared MAC address to use on both BIG-IP units in the redundant system.

The shared MAC address is used only when the BIG-IP system is in active mode. When the unit is in a standby state, the original MAC address of the network card is used.

Use the following procedure to set the MAC masquerade address that is shared by both BIG-IP units in the redundant system.

To specify a shared MAC masquerade address

1. On the Main tab of the navigation pane, expand **Network**, and click **VLANs**.
   This opens the VLANs screen, which displays a list of existing VLANs.
2. Click a VLAN name.
   This opens the properties screen for that VLAN.
3. Locate the Configuration section and select **Advanced**.
   This displays the MAC address for the first interface added to the VLAN, as well as a box for designating the MAC masquerade address.

4. Type the MAC masquerade address.
5. Click **Update**.

If you do not configure a MAC masquerade address on startup, or when transitioning from a standby state to an active state, the BIG-IP system sends gratuitous ARP requests to notify the default router and other machines on the local Ethernet segment that its MAC address has changed. See RFC 826 for more details on ARP.

Maintaining a redundant system

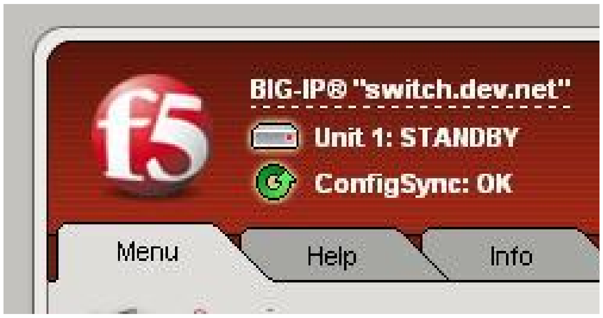
In the section titled *Before you begin*, on page 13-8, you learned how to use the Configuration utility to configure a redundant system. After you have configured your redundant system and put it into service, however, you can perform a number of tasks on a regular basis to keep the system up and running properly. These tasks are:

- Viewing the redundancy state of a unit and the synchronization state
- Changing the redundancy state of a unit
- Determining the ID of a unit
- Altering failover behavior
- Controlling failback
- Converting an active-active system to an active/standby system

Viewing redundancy states and synchronization status

You can globally view the current redundancy state of a unit by viewing the upper-left corner of any Configuration utility screen. You can also view synchronization status in this same portion of each screen, but only if you have configured the unit to do so. (For more information on viewing synchronization status, see *Viewing synchronization status*, on page 13-34.)

Figure 13.3 shows an example of the status information as displayed on a Configuration utility screen.



BIG-IP® "switch.dev.net"

Unit 1: STANDBY

ConfigSync: OK

Figure 13.3 *Viewing redundancy state and synchronization status*

Viewing redundancy state

Each unit in a redundant system is in either an active or a standby state at any given time. The current state of a unit depends on the unit's redundancy state preference, and whether the unit is available or unavailable to accept connections. You can use the Configuration utility in two different ways to determine the current state of a unit.

One way to view the redundancy state of a BIG-IP unit is by checking the status display that appears in the upper-left corner of every Configuration utility screen. See Figure 13.3, on page 13-33 for an example of this status display.

The other way to view the redundancy state of a unit is to use the following procedure.

To view the redundancy state of a unit

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. View the value of the **Current Redundancy State** setting, either **Active** or **Standby**.

Viewing synchronization status

As you learned in *Synchronizing configuration data*, on page 13-18, it is essential that an active unit share its current configuration data with its peer to ensure that failover can occur successfully. Configuration data on a unit can change for a variety of reasons (such as when adding a virtual server or modifying a profile), so it is important that you be able to monitor synchronization status at any given time, and re-synchronize the units if necessary.

You can view either detailed synchronization information about the current unit and its peer, or you can view general synchronization status on every Configuration utility screen.

Viewing detailed synchronization status

You can view detailed configuration synchronization status, such as the internal static self IP addresses that the two units use when synchronizing data, by displaying the ConfigSync screen of the Configuration utility. This screen is available from the Redundancy Properties screen.

Table 13.3 lists and describes the status-related settings that the ConfigSync screen displays.

Status Setting	Description
ConfigSync Peer	Displays the internal static self IP address that the BIG-IP system uses to determine the peer unit for synchronization.
Status message	Displays the state of the peer, that is, active or standby. May also report the status as unknown if connectivity problems exist.
Last Change (Self)	Displays the day, date, and exact time that the configuration data of the unit you are configuring was last changed.
Last Change (Peer)	Displays the day, date, and exact time that the configuration data of the peer unit was last changed.
Last ConfigSync	Displays the day, date, and exact time that a user synchronized the configuration data between the two units.

Table 13.3 *Status information on the ConfigSync screen*

◆ **Tip**

You can also display this detailed status information by enabling the auto detection feature and then clicking on the resulting synchronization status in the upper-left corner of the Configuration utility. For more information, see ***Viewing general synchronization status****, following.*

Viewing general synchronization status

The BIG-IP system can display general synchronization status in the upper-left corner of every Configuration utility screen (see Figure 13.3, on page 13-33). To use this feature, you must first enable the feature that automatically detects synchronization status. For more information on how to enable this feature, see *Performing configuration synchronization*, on page 13-19.

Once you have enabled the automatic status detection feature, the status that the Configuration utility displays indicates whether or not you need to synchronize the configurations of the two units due to changes that you might have made to the configuration data. For example, if you change the redundancy preference of unit 2, you must then synchronize the configuration so that both units are aware of the change.

The synchronization status messages that the BIG-IP system can report are:

- **ConfigSync: OK** (green circular arrow)
  No synchronization required
- **Sync Recommended** (orange/yellow circular arrow)
  Synchronize to or from the peer

- **Sync Recommended** (gray/white circular arrow)
  Manual intervention recommended
- **Unknown sync state** (gray/white circular arrow)
  State of unit is unknown due to loss of peer connection

Note that the color of the icon changes depending on the synchronization status. To see an example of general synchronization status, see Figure 13.3, on page 13-33.

◆ **Tip**

*You can view more detailed synchronization information by clicking the synchronization status that is displayed in the upper-right corner of every Configuration utility screen. You can also view this detailed information by displaying the ConfigSync screen within the Configuration utility. For more information, see **Viewing detailed synchronization status**, on page 13-34.*

Changing the redundancy state

In addition to viewing the current state of a BIG-IP unit, you can force a BIG-IP unit to switch from an active state to a standby state. This feature is useful when you need to take an active unit out of service in order to perform standard system maintenance tasks on that unit.

For active/standby configurations, the forcing of the active unit to a standby state causes its connections to fail over to the peer unit, and the normally-idle peer unit becomes active.

For active-active configurations, you cannot switch an active unit to a standby state if that unit is currently processing connections for the peer unit due to a failover.

To change the redundancy state from active to standby

To force a unit from an active to a standby state, display the Redundancy Properties screen for the unit, and click the **Force to Standby** button.

Determining the unit ID

Sometimes, you might need to know the unit ID assigned to a BIG-IP unit. A typical reason for needing this information is if you are configuring a second BIG-IP system to be part of a redundant system and want to know the unit ID of the existing redundant-system unit.

The **Unit ID** setting on the Redundancy Properties screen indicates whether a system is designated as unit **1** or unit **2** in the redundant system configuration.

You assign a unit ID to a unit of a redundant system at the time that you initially run the Setup utility on one of the BIG-IP units. For more information, see *Before you begin*, on page 13-8.

To determine the unit ID of a BIG-IP unit

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. Locate the **Unit ID** setting and view the unit ID number.

Customizing redundant-system behavior

The bigdb™ database contains a number of bigdb keys related to redundant-system behavior. You can change the values of these keys if you want to customize the way that a redundant system operates. For more information, see Appendix B, *Configuring bigdb Database Keys*.

Controlling failback

Failback is the process of a previously-unavailable unit reclaiming its normal traffic when the unit returns to an active state. The way that failback operates on a redundant system depends on whether your system is an active/standby or an active-active configuration.

When failback occurs in either an active/standby or active-active configuration, the BIG-IP system drops any connections that had previously failed over to the peer unit, unless you configured the relevant virtual server or SNAT to mirror those connections. For information on connection mirroring, see *Mirroring connection information*, on page 13-29.

◆ **Tip**

The upper-left corner of the Configuration utility screens continually reports the state of the redundant-system unit that you are currently managing (active or standby). For more information, see ***Viewing redundancy state****, on page 13-33.*

Controlling failback for active/standby mode

In a typical active/standby configuration, where no preference is set for which unit is active, failback is not automatic. If unit 1 fails over to unit 2 and later becomes available again, unit 1 remains in a standby state and unit 2 continues to process the traffic, unless you specifically initiate failback or failover occurs again. In the latter case, unit 2 fails over to unit 1.

You normally initiate failback by forcing the currently-active unit into a standby state. When you initiate failback, the BIG-IP system drops the connections that failed over from the other unit, unless you have connection mirroring enabled on the relevant virtual server or SNAT. For information on connection mirroring, see *Mirroring connection information*, on page 13-29.

As an option, you can set a state preference for a particular unit. Setting this preference automates the failback process. For example, if you specify that you prefer unit 1 to be the active unit whenever possible, then automatic failback to unit 1 occurs as soon as possible after a failover to unit 2. Automatic failback also occurs if you specify that you prefer unit 2 to be the standby unit. For information on setting a state preferences see *Specifying a redundancy state preference*, on page 13-14.

To initiate failback for an active/standby system

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.

2. At the bottom of the screen, click the **Force to Standby** button.

Controlling failback for active-active mode

Failback for an active-active configuration is never automatic, because during failback, the BIG-IP system drops the connections that failed over from the other unit, unless you have connection mirroring enabled on the relevant virtual server. For information on connection mirroring, see *Mirroring connection information*, on page 13-29.

You can, however, specifically initiate failback. In this case, failback causes the failover unit (for example, unit 2) to relinquish the processing of unit 1 traffic back to unit 1, while continuing to process its own traffic. The normal time that it takes for failback to complete on an active-active system is 60 seconds.

To initiate failback for an active-active system

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.

2. At the bottom of the screen, click the **Fail Back** button.

◆ **Note**

You can enable automatic failback by configuring the ***Common.Bigip.ManFailBack*** *bigdb database key. You can also change the number of seconds it takes for failback to occur, by configuring the* ***Failover.FailbackDelay*** *key. For more information, see Appendix B,* ***Configuring bigdb Database Keys****.*

Converting an active-active system to an active/standby system

Returning to active/standby mode from active-active mode is relatively simple in that only a few things need be changed. Use the Configuration utility to do this conversion, being sure to make these same changes on each unit of the redundant pair.

To change the redundancy mode of a redundant system

1. On the Main tab of the navigation pane, expand **System**, and click **High Availability**.
   The Redundancy Properties screen opens.
2. From the **Redundancy Mode** list, change the mode to **Active/Standby**.
3. On the menu bar, click ConfigSync.
   The ConfigSync screen opens.
4. For the **Synchronize** setting, click **Synchronize TO Peer**.
5. Click **Update**.
6. On the menu bar, click Redundancy.
   The Redundancy Properties screen opens.
7. From the **Redundancy State Preference** list, change the preferred state of the unit to **Active** or **Standby**. For more information, see *Specifying a redundancy state preference*, on page 13-14.
8. Click **Update**.

Once the system is running in active/standby mode, it is the active unit that manages connections for all local traffic management objects (such as virtual servers and SNATs), regardless of the unit associated with those objects. Therefore, it is not necessary to re-associate virtual servers, SNATS, or NATs with a specific unit when you transition from active-active mode to active/standby mode.

14

Managing User Accounts

- Introducing user account management
- Managing local user accounts
- Managing remote user accounts

Introducing user account management

An important part of managing the BIG-IP system is creating and managing user accounts for BIG-IP system administrators. By creating user accounts for system administrators, you provide additional layers of security. User accounts ensure that the system:

- Verifies the identity of users logging into the system (authentication)
- Controls user access to system resources (authorization)

To enable user authentication and authorization, you assign passwords and user roles to your user accounts. ***Passwords*** allow you to authenticate your users when they attempt to log in to the BIG-IP system. ***User roles*** allow you to control user access to BIG-IP system resources.

◆ **Note**

The entire set of user accounts that you create for BIG-IP system administrators must reside either locally on the BIG-IP system, or remotely on another type of authentication server.

The types of servers that you can use to remotely store BIG-IP system user accounts are:

- Active Directory™ servers
- Lightweight Directory Access Protocol (LDAP) servers
- Remote Authentication Dial-in User Service (RADIUS) servers

If you want your user accounts to reside locally on the BIG-IP system, you must create those user accounts on the BIG-IP system and assign user roles to them. If you want your user accounts to reside remotely on an Active Directory, LDAP, or RADIUS server, you do not use the BIG-IP system to create the accounts. Instead, you use the mechanism provided by the server vendor, and you use BIG-IP system strictly to assign user roles to those remote accounts and to maintain those user role assignments over time.

Understanding user account types

There are two types of user accounts on the BIG-IP system: System maintenance accounts and Web UI accounts.

- ◆ **System maintenance accounts**
  System maintenance accounts are user accounts that you maintain using the Setup utility. There are two types of system maintenance accounts: the **root** account and the **support** account. System maintenance accounts reside locally on the BIG-IP system and grant full access to BIG-IP system resources. You configure and maintain these accounts using the Setup utility.

- ◆ **Web UI accounts**
  Web UI accounts are user accounts that you create for other BIG-IP system administrators to use. Web UI accounts can reside either locally

on the BIG-IP system, or remotely on a remote authentication server. You create and maintain these accounts using the browser-based Configuration utility. Creating Web UI accounts allows you to assign various user roles to those accounts as a way to control system administrator access to BIG-IP system resources. A special Web UI account is the **admin** account, which automatically exists on any BIG-IP system. For more information on the **admin** account, see *Configuring the admin account*, on page 14-4. For information on user roles, see *Understanding user roles*, following.

You are not required to have any accounts other than the system maintenance accounts (**root** and **support)** and the **admin** Web UI account, but we recommend that you do so, as a way to intelligently control administrator access to system resources.

The tools you use to create and maintain user accounts vary according to the type of account you are managing. Table 14.1 lists the various user accounts for the BIG-IP system and the tools you use to manage them.

Account Name	Creation/Configuration Tool	Maintenance Tool
The **root** account	Setup utility	Setup utility
The **support** account	Setup utility	Setup utility
The **admin** account	Setup utility	Configuration utility
Other Web UI accounts	Configuration utility	Configuration utility

Table 14.1 *Tools for managing user accounts*

Understanding user roles

User roles are a means of authorization that allows you to control a user's access to BIG-IP system resources. More specifically, a ***user role*** defines the types of tasks that a user can perform on the BIG-IP system and the tools that the user can use to perform those tasks. When you create a local or remote user account, you can assign one of four user roles to that account.

Table 14.2 lists and describes the various user roles that you can assign to a user account.

User Role	Description
No Access	When a user role is set to **No Access**, the user cannot view, modify, or create any configuration information for the BIG-IP system.
Guest	The **Guest** user role grants read-only access to the user, through the Configuration utility only. A user with this user role has no access to the command-line interface. A user with the **Guest** role can view configuration information, but cannot create new objects or modify existing ones. Users with this access level do not have access to various Configuration utility elements such as **Create** buttons, **Update** buttons, and **Delete** buttons.
Operator	The **Operator** user role allows the user to view information and to enable or disable nodes. Users with this user role can access the BIG-IP system through the Configuration utility only.
Administrator	This user role provides the user with full access to all administrative tasks. By default, users with this user role can access the BIG-IP system through the Configuration utility and iControl, but not through the command line interface. However, as an option, you can assign users the ability to also access the BIG-IP system through the command-line interface.

***Table 14.2** User roles for user accounts*

The BIG-IP system automatically assigns a user role to an account when you create that account. The user role that the system assigns to a user account depends on the type of account:

- **root and admin accounts**
  The BIG-IP system automatically assigns the **Administrator** user role to the system maintenance **root** account and the Web UI **admin** account. You cannot change this user-role assignment. Thus, any user who successfully logs into the BIG-IP system using the **root** or **admin** account has full access to system resources and can perform all administrative tasks.

- **Other Web UI accounts**
  The BIG-IP system automatically assigns the **No Access** user role to all Web UI accounts other than the **admin** account. If the user account you are using has the **Administrator** role assigned to it, you can change another account's user role from **No Access** to **Guest**, **Operator**, or **Administrator**. For remote user accounts, if you know that most of your users will need some amount of access to system resources, you can configure the BIG-IP system to use a role other than **No Access** as the default user role.

Managing local user accounts

Managing local user accounts refers to the tasks of creating, viewing, modifying, and deleting local Web UI user accounts on the BIG-IP system, using the browser-based Configuration utility.

The Configuration utility stores local user accounts (including user names, passwords, and user roles) in a local user-account database. When a user logs into the BIG-IP system using one of these locally-stored accounts, the BIG-IP system checks the account to determine the access level assigned to that user account.

You assign a user role to an account at the time that you create the account, or by changing the properties of an existing account.

◆ **Important**

Except for users who want to change their own passwords, only users with the role of ***Administrator*** *can manage local user accounts.*

Configuring the admin account

A user account called **admin** resides on every BIG-IP system. Although the BIG-IP system creates this account automatically, you must still assign a password to the account before you can use it. To initially set the password for the **admin** account, you must run the Setup utility. To change its password later, you use the Configuration utility's Users screens.

The **admin** account resides in the local user account database on the BIG-IP system. By default, the BIG-IP system assigns the **Administrator** user role, which gives the user of this account full access to all BIG-IP system resources. You cannot change the user role on this account. For information on user roles, see *Understanding user roles*, on page 14-2.

Configuring a secure password policy

The BIG-IP system includes an optional administrative feature: a security policy for creating passwords for local BIG-IP system user accounts. A secure password policy ensures that BIG-IP system users that have local user accounts create and maintain passwords that are as secure as possible.

The secure password policy feature includes two distinct types of password restrictions:

- **Enforcement restrictions**
  These are, specifically, character restrictions that you can enable or disable. They consist of the minimum password length and the required character types (numeric, upper case, lower case, and other kinds of characters). When enabled, enforcement restrictions are applied only to user accounts with **Guest** and **Operator** roles, and are never enforced on user accounts that have the **Administrator** role assigned to them.

Consequently, a user with **Administrator** permissions does not need to adhere to these restrictions when either changing his or her own password, or changing the passwords of other user accounts.

- **Policy restrictions**
  These restrictions represent the minimum and maximum lengths of time that passwords can be in effect. Also included in this type of policy restriction are the number of days prior to password expiration that users are warned, and the number of previous passwords that the BIG-IP system should store, to prevent users from re-using former passwords. Policy restrictions apply to all user accounts, regardless of user role assigned to them. These restrictions are always enabled, although using the default values provides a minimal amount of restriction.

The password policy feature affects passwords for local user accounts only. Passwords for remotely-stored user accounts are not subject to this local password policy, but might be subject to a separate password policy defined on the remote system.

◆ **Important**

You must have the user role of ***Administrator*** *assigned to your account to configure this feature.*

Table 14.3 shows the settings that you can configure, along with their descriptions and default values.

Setting	Description	Default Value
Secure Password Enforcement	Enables or disables character restrictions, that is, a policy for minimum password length and required characters. When you enable this setting, the Configuration utility displays the **Minimum Length** and **Required Characters** settings.	**Disabled**
Minimum Length	Specifies the minimum number of characters required for a password, and the allowed range of values is **6** to **255**. This setting appears only when you enable the **Secure Password Enforcement** setting. ***Important:*** *When enabled, this setting is enforced only on user accounts with the* ***Guest*** *and* ***Operator*** *roles assigned to them; any user account with the* ***Administrator*** *role assigned to it (including the* **root**, **support**, and **admin** *accounts) is not subject to the restrictions imposed by this setting.*	**6**

Table 14.3 *Configuration settings for a secure password policy*

Setting	Description	Default Value
Required Characters	Specifies the number of numeric, upper case, lower case, and other characters required for a password. The allowed range of values is **0** to **127**. This setting appears only when you enable the **Secure Password Enforcement** setting. ***Important:*** *When enabled, this setting is enforced only on user accounts with the **Guest** and **Operator** roles assigned to them; any user account with the **Administrator** role assigned to it (including the* **root**, **support**, and **admin** *accounts) is not subject to the restrictions imposed by this setting.*	**0**
Password Memory	Specifies, for each user account, the number of former passwords that the BIG-IP system retains to prevent the user from re-using a recent password. The range of allowed values is **0** to **127**. This setting applies to all user accounts.	**0**
Minimum Duration	Specifies the minimum number of days before a user can change a password. The range of allowed values is **6** to **255**. This setting applies to all user accounts.	**6**
Maximum Duration	Specifies the maximum number of days that a user's password can be valid. The range of allowed values is **1** to **99999**. This setting applies to all user accounts.	**99999**
Expiration Warning	Specifies the number of days prior to password expiration that the system sends a warning message to a user. The range of allowed values is **1** to **255**. This setting applies to all user accounts.	**7**

Table 14.3 *Configuration settings for a secure password policy*

To configure the password policy feature

1. On the Main tab on the navigation pane, expand **System**, and click **Users.**
   The Users screen opens.

2. From the menu bar, click **Authentication**.
   This displays the screen for implementing a password policy.

3. Under Password Policy, locate the Secure Password Enforcement setting and set it to meet your needs:

   a) If you want to enable character restrictions for **Guest** and **Operator** accounts, locate the **Secure Password Enforcement** setting and select **Enabled.**
   This displays the **Minimum Length** and **Restrictions** settings on the screen. Retain or change the values for these settings.

   b) If you do not want to enable character restrictions for **Guest** and **Operator** accounts, leave the **Secure Password Enforcement** setting set to **Disabled**.

4. Retain the default values for all other settings, or change them to suit your needs.
   These settings represent the secure password policy restrictions, which apply to all user accounts, regardless of user role.
5. Click **Finished**.

◆ **Note**

Whenever you change the secure password policy, the new configuration values, such as password expiration, do not apply to passwords that were created prior to the policy change. However, the new policy takes effect the next time that the user changes his or her password.

Creating user accounts

When you create a local user account, you must give the account a name and a password. You must also set the user role, either by retaining the default user role or by assigning a new one. The default user role for local, non-system accounts is **No Access**.

Only users who have been granted the **Administrator** role can create user accounts.

To create a user account

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all Web UI accounts.
2. In the upper right corner of the screen, click **Create**.
   The New User screen opens.
3. In the **User Name** box, type a name for the user account.
4. For the **Authentication** setting, type and confirm a password for the account.
   For more information on user account passwords, see *Managing remote user accounts*, on page 14-11.
5. To grant an access level other than **No Access**, use the **Web User Role** setting and select one of these options:
   - **Administrator**
     You can optionally check the **Allow Console Access** box, which grants access to the BIG-IP system through the command line interface.
   - **Operator**
   - **Guest**
6. Click **Finished**.

Viewing user accounts

Using the Configuration utility, you can easily display a list of existing local user accounts and view the properties of an individual account. Only users who have been granted the **Administrator** role can view the settings of other user accounts.

To display a list of existing user accounts

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all Web UI accounts.
2. View the list of user accounts.

To view the properties of a user account

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all Web UI accounts.
2. In the user-account list, find the user account you want to view and click the account name.
   This displays the properties of that user account.

Modifying user accounts

You use the Configuration utility to modify the properties of any existing local user account, other than the **root** account. Only users who have been granted the **Administrator** role can modify user accounts other than their own.

When you modify account properties, you can:

- Change the password
- Change the user role
- Allow console access (that is, using SSH) if the account has a user role of **Administrator**

Users with user roles of **Operator** or **Guest** can change their own passwords only. Users with an **Administrator** role can change their own passwords as well as other users' passwords.

To change properties of a user account other than root

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   The User List screen opens, displaying a list of all Web UI accounts.
2. In the user-account list, click a user account name.
   This displays the properties of that account.

3. Change the password, or choose a new user role for the account, or both. If the user account has the **Administrator** role assigned to it, or you are changing the user role to **Administrator**, you can optionally check the **Allow Console Access** box.
4. Click **Update**.

You can also change some properties of the **root** account. Specifically, you can change the password of the **root** account, and you can enable or disable access to the BIG-IP system through SSH.

To change properties of the root account

1. On the Main tab of the navigation pane, expand **System**, and click **Platform**.
   The General screen opens.
2. For the **Root Account** setting, type a new password in the **Password** box, and re-type the new password in the **Confirm** box.
3. If you want to grant SSH access, then for the **SSH Access** setting, check the **Enabled** box, and for the **SSH IP Allow** setting, either:
   - Select *** All Addresses**.
   - Select **Specify Range** and type a range of IP addresses.
4. Click **Update**.

◆ **Important**

If you have a redundant system configuration and you change the password on the ***admin*** *account, you must also change the password on the peer unit, to ensure that synchronization of configuration data operates correctly.*

Deleting user accounts

If the account you are using has an **Administrator** user role, you can delete other local user accounts. When you delete a local user account, you remove it permanently from the local user-account database on the BIG-IP system.

◆ **Note**

You cannot delete the ***admin*** *user account, nor can you delete the user account with which you are logged in.*

To delete a user account

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all Web UI accounts.
2. In the user-account list, locate the name of the account you want to delete and click the Select box to the left of the account name.

3. Click the **Delete** button.
   A confirmation box appears.
4. Click **Delete** again.

Managing remote user accounts

Rather than store your administrative Web UI accounts locally on the BIG-IP system, you can instead store them on a remote authentication server. In this case, you create all of your Web UI accounts (including user names and passwords) on that remote server, using the mechanism supplied by that server's vendor.

Authentication for remote user accounts is based on standard HTTP authentication, that is, user name and password. The exception to this is when the remote server is specifically configured to perform SSL authentication. In this case, authentication is based on SSL certificates.

Once you have created the user accounts on the remote server, you then use the BIG-IP system to assign user roles to those accounts, for the purpose of controlling user access to BIG-IP system resources.

You assign user roles to remote accounts using the Configuration utility. The Configuration utility stores user-role information in the BIG-IP system's local user-account database. When a user whose account information is stored remotely logs into the BIG-IP system and is granted authentication, the BIG-IP system then checks its local database to determine the user role that you assigned to that user.

If you do not assign a user role to a remote user account, then the BIG-IP system assigns a default user role. You can specify which user role you want the BIG-IP system to assign as a default user role. For more information, see *To configure the default user role*, on page 14-16.

◆ **Important**

Only users with the role of ***Administrator*** *can manage user roles for remote user accounts.*

Specifying a remote user-account database

One of the tasks you perform with the Configuration utility is to specify the type of remote user-account database that currently stores your remote user accounts. The available database types that you can specify are:

- Microsoft® Windows Active Directory
- Lightweight Directory Access Protocol (LDAP)
- Remote Authentication Dial-In User Service (RADIUS)

When you specify the type of remote database, you can also configure some database settings. Then, once you have configured the remote user account database, you can assign user roles to your remote user accounts. For more information on user roles, see *Assigning user roles*, on page 14-14.

If the remote authentication server is an Active Directory or LDAP server and is set up to authenticate SSL traffic, there is an additional feature that you can enable. You can configure the BIG-IP system to perform the server-side SSL handshake that the remote server would normally perform when authenticating client traffic. In this case, there are some preliminary steps you must perform to prepare for remote authentication using SSL.

To prepare for SSL-based remote authentication

1. Convert the Certificate Authority (CA) or self-signed certificates to PEM format.
2. On the BIG-IP system, import the certificates, using the Configuration utility.
   You can store the certificates in any location on the BIG-IP system. For information on importing certificates, see the ***Network and System Management Guide***.

Once you have performed these preliminary SSL tasks, you can enable SSL as part of the procedure described in *To configure remote Active Directory or LDAP authentication*, following.

If the remote server is a RADIUS server, see *To configure remote RADIUS authentication*, on page 14-13.

To configure remote Active Directory or LDAP authentication

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   The Users screen opens.
2. On the menu bar, click **Authentication Source**.
   The Authentication Source screen opens.
3. Click **Change**.
4. From the **User Directory** list, select **Remote - Active Directory** or **Remote - LDAP**.
5. In the **Host** box, type the IP address of the remote server.
6. For the **Port** setting, retain the default port number (**389**) or type a new port number in the box.
   This setting represents the port number that the BIG-IP system uses to access the remote server.
7. In the **Remote Directory Tree** box, type the file location (tree) of the user authentication database on the Active Directory or LDAP server. At minimum, you must specify a domain component (that is, **dc=<value>**).
8. For the **Scope** setting, retain the default value (**Sub**) or select a new value.
   This setting specifies the level of the remote server database that the BIG-IP system should search for user authentication. For more information on this setting, see the online help.

9. For the **Bind** setting, specify a user ID login for the remote server:

   a) In the **DN** box, type the Distinguished Name for the remote user ID.

   b) In the **Password** box, type the password for the remote user ID.

   c) In the **Confirm** box, re-type the password that you typed in the Password box.

10. If you want to enable SSL-based authentication, click the **SSL** box and if necessary, configure the following settings.

    Important: *Be sure to specify the full path name of the storage location on the BIG-IP system. For example, if the certificate is stored in the directory* ***/config/bigconfig/ssl.crt****, type the value* ***/config/bigconfig/ssl.crt****.*

    a) In the **SSL CA Certificate box**, type the name of a chain certificate, that is, the third-party CA or self-signed certificate that normally resides on the remote authentication server.

    b) In the **SSL Client Key** box, type the name of the client SSL key. Use this setting only in the case where the remote server requires that the client present a certificate. If a client certificate is not required, you do not need to configure this setting.

    c) In the **SSL Client Certificate** box, type the name of the client SSL certificate.
    Use this setting only in the case where the remote server requires that the client present a certificate. If a client certificate is not required, you do not need to configure this setting.

11. Click **Finished**.

To configure remote RADIUS authentication

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   The Users screen opens.

2. On the menu bar, click **Authentication Source**.
   The Authentication Source screen opens.

3. Click **Change**.

4. From the **User Directory** list, select **Remote - RADIUS**.

5. For the **Primary** setting, configure these settings:

   a) In the **Host** box, type the IP address of the remote server.

   b) In the **Port** box, retain the default port number (**1812**) or type a new port number in the box.
   This setting represents the port number that the BIG-IP system uses to access the remote server.

   c) In the **Secret** box, type the RADIUS secret.

d) In the **Confirm** box, re-type the secret that you typed in the **Secret** box.
Note that the values of the **Secret** and **Confirm** settings must match.

6. If you want to configure a secondary RADIUS server in the event that the primary server becomes unavailable, locate the **Secondary** setting and check the **Configure Secondary Host** box.
This causes additional settings to appear.
7. Configure the remaining settings for the secondary server, using the instructions for the primary server in step 5.
8. Click **Finished**.

Assigning user roles

You create remote user accounts using the mechanism provided by the vendor of your remote server. Once you have created remote accounts, you then use the Configuration utility to assign user roles to those accounts. More specifically, you can use the Configuration utility to:

- Explicitly assign a user role to an individual remote account
- Change the user role of an account
- Specify a default user role for accounts that do not have explicit user-role designations

Explicitly assigning a user role

As stated in the previous section, you do not use the Configuration utility to create remote user accounts for the BIG-IP system. However, you can use the Configuration utility to explicitly assign user roles to them.

This task of assigning a user role to a remote account is not required, because the BIG-IP system automatically assigns a default user role to a remote account if you do not explicitly do so. For information on configuring the default user role, see *Configuring the default user role*, on page 14-15.

To explicitly assign a user role

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
This opens the User List screen, displaying a list of all user accounts.

   Note: *This list shows only the remote accounts to which you have explicitly assigned a user role. For more information, see Changing a user role, on page 14-15.*

2. In the upper-right corner of the screen, click **Create**.
This displays the New User screen.

3. In the **User Name** box, type the name of the remote user to which you want to assign a user role.
4. For the **Web User Role** setting, select a user role.
   If you select **Administrator**, the **Allow Console Access** setting appears.
5. If you selected **Administrator** and want to allow access to the BIG-IP system through the command line interface, click the **Allow Console Access** box.
6. Click **Finished**.

Changing a user role

Sometimes you might want to change the user role that you previously assigned to a remote account. To do so, you must change the properties of that account by clicking the account name on the User List screen. Only those remote user accounts to which you have explicitly assigned a user role (using the Configuration utility) appear in the list of user accounts.

If you did not explicitly assign a user role to an account, the account does not appear in the list of user accounts, In this case, you cannot change the authorization properties of that individual account. For more information, see *To explicitly assign a user role*, on page 14-14.

To change the properties of a remote user account

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of user accounts to which you explicitly assigned user roles.
2. In the User Name column, click a user name.
   This displays the properties for that user account.
3. In the **Web User Role** box, select a user role.
4. Click **Update**.

Configuring the default user role

Sometimes, you might have remote user accounts to which you have not explicitly assigned user roles. (For more information, see *Assigning user roles*, on page 14-14.) Such accounts do not appear in the list of user accounts on the User List screen.

To ensure that these accounts have a user role assigned to them, the BIG-IP system automatically assigns a default user role, to ensure valid user authorization. By default, the user role that the BIG-IP system assigns to these remote accounts is **No Access**. However, you can change the user role that the BIG-IP system uses as the default user role, to **Administrator**,

Operator, or **Guest**. Then, whenever you create a user account on that remote server and you do not explicitly assign a user role to that account, the BIG-IP system automatically assigns that user role to the account.

To configure the default user role

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all Web UI accounts.
2. From the Users menu, choose Remote Access.
   This displays the Remote Access screen.
3. In the **Web User Role** setting, select a default user role from the list.
   If you select the **Administrator** user role, an optional setting appears for granting console access to the user.
4. If you want to grant the user access to the BIG-IP system through the command-line interface, check the **Allow Console Access** box.
5. Click **Update**.

At any time, you can view the default user role that the BIG-IP system assigns to any remote accounts for which you have not explicitly assigned a user role.

To view the current default user role

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all Web UI accounts.
2. From the Users menu, choose Remote Accounts.
   The **Web User Role** setting displays the user role that the BIG-IP system currently uses as the default user role for remote accounts.

Deleting an explicit user-role designation

When you use the Configuration utility to delete a remote user account, you are not actually deleting the account from the remote server. Instead, you are removing the explicit user-role designation that you previously assigned the account.

Removing an explicit user-role designation from a remote user account causes the BIG-IP system to assign the default user role to the account.

To delete an explicit user role designation

1. On the Main tab of the navigation pane, expand **System**, and click **Users**.
   This opens the User List screen, displaying a list of all Web UI accounts.

2. Locate an account name in the list and click the corresponding Select box.
3. Click **Delete**.
   A confirmation page appears.
4. Click **Delete**.

15

Configuring SNMP

- Introducing SNMP administration
- Configuring the SNMP agent
- Working with SNMP MIB files
- Collecting performance data

Introducing SNMP administration

Simple Network Management Protocol (SNMP) is an industry-standard protocol that gives a standard SNMP management system the ability to remotely manage a device on the network. One of the devices that an SNMP management system can manage is a BIG-IP system. The SNMP versions that the BIG-IP system supports are: SNMP v1, SNMP v2c, and SNMP v3. The BIG-IP system implementation of SNMP is based on a well-known SNMP package, Net-SNMP, which was formerly known as UCD-SNMP.

Reviewing an industry-standard SNMP implementation

A standard SNMP implementation consists of an ***SNMP manager,*** which runs on a management system and makes requests to a device, and an ***SNMP agent,*** which runs on the managed device and fulfills those requests. SNMP device management is based on the standard management information base (MIB) known as MIB-II, as well as object IDs and MIB files.

- The ***MIB*** defines the standard objects that you can manage for a device, presenting those objects in a hierarchical, tree structure.
- Each object defined in the MIB has a unique object ID (OID), written as a series of integers. An ***OID*** indicates the location of the object within the MIB tree.
- A set of MIB files resides on both the SNMP manager system and the managed device. ***MIB files*** specify values for the data objects defined in the MIB. This set of MIB files consists of standard SNMP MIB files and enterprise MIB files. ***Enterprise*** MIB files are those MIB files that pertain to a particular company, such as F5 Networks, Inc.

Typical SNMP tasks that an SNMP manager performs include polling for data about a device, receiving notifications from a device about specific events, and modifying writable object data.

Reviewing the BIG-IP system SNMP implementation

To comply with the standard SNMP implementation, the BIG-IP system includes both an SNMP agent, a set of standard SNMP MIB files, and a set of enterprise MIB files (those that are specific to the BIG-IP system). The enterprise MIB files typically reside on both the BIG-IP system and system running the SNMP manager. Fortunately, you can use the browser-based Configuration utility to download the enterprise MIB files to your SNMP manager.

Using the BIG-IP system implementation of SNMP, the SNMP manager can perform these distinct functions:

- Poll for information (such as performance metrics)
- Receive notification of specific events that occur on the BIG-IP system
- Set data for SNMP objects that have a read/write access type

The last item in the list refers to the ability of an SNMP manager system to enable or disable various BIG-IP system objects such as virtual servers and nodes. Specifically, you can use SNMP to:

- Enable or disable a virtual server
- Enable or disable a virtual address
- Enable or disable a node
- Enable or disable a pool member
- Set a node to an **up** or **down** state
- Set a pool member to an **up** or **down** state
- Reset statistical data for all BIG-IP objects

Summarizing SNMP configuration on the BIG-IP system

Before an SNMP manager system can manage a BIG-IP system remotely, you must perform a few configuration tasks on the BIG-IP system, using the BIG-IP system's Configuration utility. After you have performed these configuration tasks, you can use standard SNMP commands on the remote manager system to manage the BIG-IP system.

The configuration tasks you perform are:

- ◆ **Configuring the SNMP agent**
  There are a number of things you can do to configure the SNMP agent on the BIG-IP system. For example, you can allow client access to information that the SNMP agent collects, and you can configure the way that the SNMP agent handles SNMP traps. ***Traps*** are definitions of unsolicited notification messages that the BIG-IP alert system and the SNMP agent send to the SNMP manager when certain events occur.

- ◆ **Downloading MIB files**
  You can download two sets of MIB files to your remote manager system: the standard SNMP MIB files and the enterprise MIB files.

Configuring the SNMP agent

To configure the SNMP agent on the BIG-IP system, you can use the Configuration utility. Configuring the SNMP agent means performing the following tasks:

- **Configuring BIG-IP system information**
  Specify a system contact name and the location of the BIG-IP system.
- **Configuring client access to the SNMP agent**
  Configure the BIG-IP system to allow access to the SNMP agent from an SNMP manager system.
- **Controlling access to SNMP data**
  Assign access levels to SNMP communities or users, to control access to SNMP data.
- **Configuring Traps**
  Enable or disable traps and specify the destination SNMP manager system for SNMP traps.

An alternative way to configure the SNMP agent is by editing certain BIG-IP system configuration files directly. These files are:

- **/config/snmp/snmpd.conf**
  This file contains most of the configuration information for the SNMP agent, including trap information.
- **/config/net-snmp/snmpd.conf**
  Required for SNMP v3 only, this file contains SNMP user names.
  Important: You must stop the **snmpd** service prior to editing this file.
- **/etc/hosts.allow**
  This file contains the IP addresses and netmasks for the manager systems that are allowed access to the BIG-IP system.

◆ **WARNING**

You should attempt to edit these files directly only if you are an advanced BIG-IP system administrator. Also, do not attempt to configure any bigdb^{TM} database keys that correspond to SNMP. Doing so could harm your system.

Configuring BIG-IP system information

You can use the Configuration utility to configure the following information:

- **Contact Information**
  The contact information is a MIB-II simple string variable defined by almost all SNMP boxes. The contact name usually contains a user name, as well as an email address.

- **Machine Location**
  The machine location is a MIB-II variable that almost all machines support. It is a simple string that defines the location of the machine.

To configure system information

1. On the Main tab of the navigation pane, expand **System**, and click **SNMP**.
   This opens the SNMP Agent Configuration screen.
2. In the Global Setup area, fill in the boxes.
   For more information, see the online help.
3. Click **Update**.

Configuring client access

An SNMP ***client*** refers to any system running the SNMP manager software for the purpose of remotely managing the BIG-IP system. To set up client access to the BIG-IP system, you specify the IP or network addresses (with netmask as required) from which the SNMP agent can accept requests. (By default, SNMP is enabled only for the BIG-IP system loopback interface, **127.0.0.1**.)

To allow client access to the SNMP agent

1. On the Main tab of the navigation pane, expand **System**, and click **SNMP**.
   This opens the SNMP Agent Configuration screen.
2. For the **Client Allow List Type** setting, select **Host** or **Network**, depending on whether the IP address you specify is a host system or a subnet.
3. Type the following information:
   - In the **Address** box, type an IP address or network address from which the SNMP agent can accept requests.
   - If you selected **Network** in step 3, type the netmask in the **Mask** box.
4. Click the **Add** button to add the host or network address to the list of allowed clients.
5. Click **Update**.

Controlling access to SNMP data

To better control access to SNMP data, you can assign an access level to an SNMP v1 or v2c community, or to an SNMP v3 user.

There is a default access level for communities, and this access level is read-only. This means that you cannot write to an individual data object that has a read/write access type until you change the default read-only access level of the community or user.

The way to modify this default access level is by using the Configuration utility to grant read/write access to either a community (for SNMP v1 and v2c) or a user (SNMP v3), for a given OID.

When you set the access level of a community or user to read/write, and an individual data object has a read-only access type, access to the object remains read-only. In short, the access level or type that is the most secure takes precedence when there is a conflict. Table 15.1 illustrates this point.

If the access type of an object is...	And you set the access level of a community or user to...	Then access to the object is...
Read-only	Read-only	Read-only
	Read/write	Read-only
Read/write	Read-only	Read-only
	Read/write	Read/write

Table 15.1 *Access control for SNMP data*

To grant community access to SNMP data (v1 or v2c only)

1. On the Main tab of the navigation pane, expand **System**, and click **SNMP**.
   This opens the SNMP Agent Configuration screen.

2. From the Agent menu, choose Access (v1, v2c).
   This displays the SNMP Access screen.

3. In the upper-right corner of the screen, click **Create**.
   This displays the New Access Record screen.

4. Select the type of address to which the access record applies, either **IPv4** or **IPv6**.

5. In the **Community** box, type the name of the SNMP community for which you are assigning an access level (in step 9).

6. In the **Source** box, type the source IP address.

7. In the **OID** box, type the OID for the top-most node of the SNMP tree to which the access applies.

8. For the **Access** setting, select an access level, either **Read Only** or **Read/Write**. (This access level applies to the community name you specified in step 6.)
9. Click **Finished**.

To grant access to SNMP data (v3 only)

1. On the Main tab of the navigation pane, expand **System**, and click **SNMP**.
   This opens the SNMP Agent Configuration screen.
2. From the Agent menu, choose Access (v3).
   This displays the SNMP Access screen.
3. In the upper-right corner of the screen, click **Create**.
   This displays the New Access Record screen.
4. In the **User Name** box, type a user name for which you are assigning an access level (in step 9).
5. For the **Authentication** setting, select a type of authentication to use, and then type and confirm the user's password.
6. For the **Privacy** setting, select a privacy protocol, and then do *one* of the following:
   - Type and confirm the user's password.
   - Click the **Use Authentication Password** box.
7. In the **OID** box, type the object identifier (OID) for the top-most node of the SNMP tree to which the access applies.
8. For the **Access** setting, select an access level, either **Read Only** or **Read/Write**. (This access level applies to the user name that you specified in step 5.)
9. Click **Finished**.

When you use the Configuration utility to assign an access level to a community or user, the utility updates the **snmpd.conf** file, assigning only a single access setting to the community or user. There might be times, however, when you want to configure more sophisticated access control. To do this, you must edit the **/config/snmp/snmpd.conf** file directly, instead of using the Configuration utility.

For example, Figure 15.1 shows a sample **snmpd.conf** file when you use the Configuration utility to grant read/write access to a community.

```
rocommunity public default

rwcommunity public1 127.0.0.1  .1.3.6.1.4.1.3375.2.2.10.1
```

Figure 15.1 *Sample access-control assignments in the* ***snmpd.conf*** *file*

In this example, the string **rocommunity** identifies a community named **public** as having the default read only access level (indicated by the strings **ro** and **default**). This read only access level prevents any allowed SNMP manager in community **public** from modifying a data object, even if the object has an access type of read/write.

The string **rwcommunity** identifies a community named **public1** as having a read/write access level (indicated by the string **rw**). This read/write access level allows any allowed SNMP manager in community **public1** to modify a data object under the tree node**.1.2.6.1.4.1.3375.2.2.10.1** (**ltmVirtualServ**) on the local host **127.0.0.1**, if that data object has an access type of read/write.

For more information, see the man page for the **snmpd.conf** file.

Configuring traps

On the BIG-IP system, ***traps*** are definitions of unsolicited notification messages that the BIG-IP alert system and the SNMP agent send to the SNMP manager when certain events occur on the BIG-IP system. Configuring SNMP traps on a BIG-IP system means configuring the way that the BIG-IP system handles traps, as well as setting the destination for notifications that the alert system and the SNMP agent send to an SNMP manager.

The BIG-IP system stores traps in two specific files:

- **/etc/alertd/alert.conf**
  Contains default SNMP traps.

  Important: Do not add or remove traps from the **/etc/alertd/alert.conf** file.
- **/config/user_alert.conf**
  Contains user-defined SNMP traps.

You use the Configuration utility to configur e traps, that is, enable traps and set trap destinations. When you configure traps, the BIG-IP system automatically updates the **alert.conf** and **user_alert.conf** file.

Enabling traps for specific events

You can configure the SNMP agent on the BIG-IP system to send, or refrain from sending, notifications when the following events occur:

- The SNMP agent on the BIG-IP system stops or starts. By default, this trap is enabled.
- The BIG-IP system receives an authentication warning, generated when a client system attempts to access the SNMP agent. By default, this trap is disabled.
- The BIG-IP system receives any type of warning. By default, this trap is enabled.

To enable traps for specific events

1. On the Main tab of the navigation pane, expand **System**, and click **SNMP**.
   This opens the SNMP Agent Configuration screen.
2. From the Traps menu, choose Configuration.
   This displays the SNMP Trap Configuration screen.
3. To send traps when someone starts or stops the SNMP agent, verify that the **Agent Start/Stop** box is checked.
4. To send notifications when authentication warnings occur, click the **Agent Authentication** box.
5. To send notifications when certain warnings occur, verify that the **Device** box is checked.
6. Click **Update**.

Setting the trap destination

In addition to enabling certain traps for certain events, you must specify the destination SNMP manager to which the BIG-IP system should send notifications. For SNMP versions 1 and 2c only, you specify a destination system by providing the community name to which the BIG-IP system belongs, the IP address of the SNMP manager, and the target port number of the SNMP manager.

◆ **Important**

If you are using SNMP V3 and want to configure a trap destination, you do not use the SNMP screens within the Configuration utility. Instead, you configure the ***snmpd.conf*** *file. For more information, see the man page for the* ***snmpd.conf*** *file.*

To specify a trap destination

1. On the Main tab of the navigation pane, expand **System**, and click **SNMP**.
   This opens the SNMP Agent Configuration screen.
2. From the Traps menu, choose Destination.
   This displays the SNMP Destination screen.
3. In the upper-right corner of the screen, click **Create**.
   This displays the New Trap Record screen.
4. For the **Version** setting, select an SNMP version number.
5. In the **Community** box, type the community name for the SNMP agent running on the BIG-IP system.
6. In the **Destination** box, type the IP address of the SNMP management system.

7. In the **Port** box, type the SNMP management system port number that is to receive the traps.
8. Click **Finished**.

Working with SNMP MIB files

As described earlier, ***MIB files*** define the SNMP data objects contained in the SNMP MIB. There are two sets of MIB files that typically reside on the BIG-IP system and the SNMP manager system: enterprise MIB files (that is, F5-specific MIB files) and standard SNMP MIB files.

Both sets of MIB files are already present on the BIG-IP system, in the directory **/usr/share/snmp/mibs**. However, you still need to download them to your SNMP manager system. You can download these MIB files from the Welcome screen of the browser-based Configuration utility. For more information, see *Downloading SNMP MIB files* on this page.

The implementation of the Packet Velocity® ASIC (PVA) feature affects the ability for users to use MIB-II to gather certain kinds of data. For example, with a PVA system, you can use MIB-II to collect statistics on physical system interfaces, but not on logical interfaces (that is, VLANs).

To make MIB-II as clear as possible, we have implemented the SNMP feature so that you use MIB-II for gathering standard Linux data only. You cannot use MIB-II to gather data that is specific to the BIG-IP system and instead must use the F5 enterprise MIB files. All OIDS for BIG-IP system data are contained in the F5 enterprise MIB files, including all interface statistics (**1.3.6.1.4.1.3375.2.1.2.4** (**sysNetwork.sysInterfaces**)).

◆ **Note**

All BIG-IP system statistics are defined by 64-bit counters. Thus, because only SNMP v2c supports 64-bit counters, your management system needs to use SNMP v2c to query BIG-IP system statistics data.

Downloading SNMP MIB files

The enterprise MIB files that you can download to the SNMP manager system are:

- **F5-BIGIP-COMMON-MIB.txt**
  This MIB file contains common information and all notifications (traps). For more information, see *Using the F5-BIGIP-COMMON-MIB.txt file*, on page 15-11.

- **F5-BIGIP-LOCAL-MIB.txt**
  This is an enterprise MIB file that contains specific information for properties associated with specific BIG-IP system features related to local traffic management (such as virtual servers, pools, and SNATs). For more information, see *Using the F5-BIGIP-LOCAL-MIB.txt file*, on page 15-12.

- **F5-BIGIP-SYSTEM-MIB.txt**.
  The **F5-BIGIP-SYSTEM-MIB.txt** MIB file includes global information on system-specific objects. For more information, see *Using the F5-BIGIP-SYSTEM-MIB.txt file*, on page 15-13.

To view the set of standard SNMP MIB files that you can download to the SNMP manager system, list the contents of the BIG-IP system directory **/usr/share/snmp/mibs.**

To download MIB files

1. On the Main tab of the navigation pane, expand **Overview**, and **c**lick **Welcome**.
   This opens the Welcome screen.
2. Scroll to the Downloads section, and locate the **SNMP MIBs** section.
3. Click the type of MIB files to download.
   The two MIB file types are F5 MIB files and Net-SNMP MIB files.
4. Follow the instructions on the screen to complete the download.

Understanding the enterprise MIB files

Once you have downloaded all of the necessary MIB files, you should familiarize yourself with the contents of the enterprise MIBs, for purposes of managing the BIG-IP system and troubleshooting BIG-IP system events.

◆ **Note**

*To manage a BIG-IP system with SNMP, you need to use the standard set of SNMP commands. For information on SNMP commands, consult your favorite third-party SNMP documentation, or visit the web site **http://net-snmp.sourceforge.net**.*

As mentioned in *Downloading SNMP MIB files*, on page 15-10, the BIG-IP system includes a set of enterprise MIB files:

- **F5-BIGIP-COMMON-MIB.txt**
- **F5-BIGIP-LOCAL-MIB.txt**
- **F5-BIGIP-SYSTEM-MIB.txt**

These MIB files contain information that you can use for your remote management station to: poll the SNMP agent for BIG-IP system-specific information, receive BIG-IP system-specific notifications, or set BIG-IP system data.

Using the F5-BIGIP-COMMON-MIB.txt file

The **F5-BIGIP-COMMON-MIB.txt** file is an enterprise MIB file that contains objects pertaining to any common information, as well as the F5-specific SNMP traps.

All F5-specific traps are contained within this MIB file. You can identify the traps within this MIB file by viewing the file and finding object names that show the designation **NOTIFICATION-TYPE**.

When an F5-specific trap sends a notification to the SNMP manager system, the SNMP manager system receives a text message describing the event or problem that has occurred. For troubleshooting assistance regarding F5-specific traps, see Appendix A, *Troubleshooting SNMP Traps*.

To see all available MIB objects in this MIB file, you can view the **F5-BIGIP-COMMON-MIB.txt** file in the directory **/usr/share/snmp/mibs** on the BIG-IP system.

Using the F5-BIGIP-LOCAL-MIB.txt file

The **F5-BIGIP-LOCAL-MIB.txt** file is an enterprise MIB file that contains information that an SNMP manager system can access for the purpose of managing local application traffic. For example, you can:

- View the maximum number of entries that a node can have open at any given time.
- Get a pool name.
- View the current active members for a load balancing pool.
- Reset pool statistics
- Get profile information such as the total number of concurrent authentication sessions.

In general, you can use this MIB file to get information on any local traffic management object (virtual servers, pools, nodes, profiles, SNATs, health monitors, and iRules). You can also reset statistics for any of these objects.

To see all available enterprise MIB objects for local traffic management, you can view the **F5-BIGIP-LOCAL-MIB.txt** file in the directory **/usr/share/snmp/mibs** on the BIG-IP system.

Using the F5-BIGIP-SYSTEM-MIB.txt file

The **F5-BIGIP-SYSTEM-MIB.txt** file is an enterprise MIB file that describes objects representing common BIG-IP system information. Examples of information in this MIB file are global statistic data, network information, and platform information. Some of the data in this MIB file is similar to that defined in MIB-II, but is not exactly the same.

Table 15.2 shows standard MIB-II objects and the F5-specific objects that approximately correspond to them.

MIB-II Category or Object	F5-BIGIP-SYSTEM-MIB Object Name
MIB-II	f5.bigipSystem
interfaces	sysNetwork.sysInterfaces.sysInterface sysNetwork.sysInterfaces.sysInterfaceStat sysNetwork.sysInterfaces.sysInterfaceMediaOptions
ip	sysGlobalStats.sysGlobalIpStat
ip.AddrTable	sysNetwork.sysSelfIp
ip.RouteTable	sysNetwork.sysRoute
ip.ipNetToMediaTable	sysNetwork.sysArpNdp
icmp	sysGlobalStats.sysGlobalIcmpStat
tcp	sysGlobalStats.sysGlobalTcpStat
udp	sysGlobalStats.sysGlobalUdpStat

Table 15.2 *F5-BIGIP-SYSTEM-MIB objects and their relationship to MIB-II objects*

MIB-II Category or Object	F5-BIGIP-SYSTEM-MIB Object Name
transmission/dot3.dot3StatTable transmission/dot3.dot3CollTable	sysNetwork.sysTransmission.sysDot3Stat
dot1dBridge.dot1dBase	sysNetwork.sysDot1dBridge
dot1dBridge.dot1dStp	sysNetwork.sysSpanningTree.sysStpBridgeStat sysNetwork.sysSpanningTree.sysStpBridgeTreeStat sysNetwork.sysSpanningTree.sysInterfaceStat sysNetwork.sysSpanningTree.sysInterfaceTreeStat
dot1dBridge.dot1dTp	sysGlobalAttr.VlanFDBTimeout
dot1dBridge.dot1dTpFdbTable	sysNetwork.sysL2
dot1dTpPortTable	sysNetwork.sysInterfaces.sysInterfaceStat
dot1dStaticTable	Not supported.
ifMIB/ifMIBObjects.ifXTable	sysNetwork.sysInterfaces.sysIfxStat

Table 15.2 *F5-BIGIP-SYSTEM-MIB objects and their relationship to MIB-II objects*

To see all available enterprise MIB system objects, you can view the **F5-BIGIP-SYSTEM-MIB.txt** file in the directory **/usr/share/snmp/mibs** on the BIG-IP system.

Using the RMON-MIB.txt file

One of the MIB files that the BIG-IP system provides is the Remote network Monitoring (RMON) MIB file, **RMON-MIB.txt**. This file is the standard RMON MIB file. However, the implementation of RMON on the BIG-IP system differs slightly from the standard RMON implementation, in these ways:

- The BIG-IP system implementation of RMON supports four of the nine RMON groups. The four supported RMON groups are: statistics, history, alarms, and events.
- The **RMON-MIB.txt** file monitors the BIG-IP system interfaces (that is, **sysIfIndex**), and not the standard LINUX interfaces.
- For hardware reasons, the packet-length-specific statistics in the RMON statistics group offer combined transmission and receiving statistics only. This behavior differs from the behavior described in the definitions of the corresponding object IDs.

To understand how RMON operates for a BIG-IP system, you can view the **RMON-MIB.txt** file in the directory **/usr/share/snmp/mibs** on the BIG-IP system.

Collecting performance data

The Configuration utility on the BIG-IP system displays graphs showing performance metrics for the system. However, you can also use SNMP to collect the same information.

The types of performance metrics that you can gather using SNMP are:

- Memory use
- Number of active connections
- Number of new connections
- Throughput in bits per second
- Number of HTTP requests
- Ram Cache use
- CPU use
- Number of SSL transactions

Each type of metric has one or more SNMP object IDs (OIDs) associated with it. To gather performance data, you specify these OIDs with the appropriate SNMP command.

For example, the following SNMP command collects data on current memory use, where **public** is the community name and **bigip** is the host name of the BIG-IP system:

```
snmpget -c public bigip sysGlobalStat.sysStatMemoryUsed.0
```

For some types of metrics, such as memory use, simply issuing an SNMP command with an OID gives you the information you need. For other types of metrics, the data that you collect with SNMP is not useful until you perform a calculation on it to interpret the data.

For example, to determine the throughput rate of client bits coming into the BIG-IP system, you must you must use the relevant OID (**sysStatClientBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.3)**) to take two polls at a certain interval (such as ten seconds), calculate the delta of the two polls, and then perform the following calculation on that delta value:

```
( <DeltaStatClientBytesIn>*8 ) / <interval>
```

◆ **Important**

For calculations that include a polling interval, the interval can be any amount of time that you choose, as long as you use that same number as the value for ***<interval>*** *in your calculations. Note that the performance graphs that the Configuration utility displays are based on a polling interval of ten seconds.*

The following sections contain tables that list:

- The OIDs that you can use to collect the performance data
- The calculations that you must perform to interpret the performance data that you collect (not required for interpreting data on memory use and active connections).

Collecting data on memory use

You can use an SNMP command with OIDs to gather data on the number of bytes of memory currently being used on the BIG-IP system. Table 15.3 shows the OIDs that you need to specify to gather data on current memory use. To interpret data on memory use, you do not need to perform a calculation on the collected data.

Performance Graph (Configuration utility)	Graph Metric	Required SNMP OIDs
Memory Used	TMM Mem Usage	sysStatMemoryUsed (.1.3.6.1.4.1.3375.2.1.1.2.1.45)
	Host Mem Usage	sysHostMemoryUsed (.1.3.6.1.4.1.3375.2.1.7.2)

Table 15.3 *Required OIDs for collecting metrics on memory use*

Collecting data on active connections

You can use SNMP commands with various OIDs to gather data on the number of active connections on the BIG-IP system. Table 15.4 shows the OIDs that you need to specify to gather data on active connections. To interpret data on active connections, you do not need to perform any calculations on the collected data.

Performance Graph (Configuration utility)	Graph Metrics	Required SNMP OIDs
Active Connections (summary graph)	Connections	sysStatClientCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.8)
Active Connections (detailed graph)	client	sysStatClientCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.8)
	server	sysStatServerCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.15)
	pva client	sysStatPvaClientCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.22)
	pva server	sysStatPvaServerCurConns (.1.3.6.1.4.1.3375.2.1.1.2.1.29)
	ssl client	sysClientsslStatCurConns (.1.3.6.1.4.1.3375.2.1.1.2.9.2)
	ssl server	sysServersslStatCurConns (.1.3.6.1.4.1.3375.2.1.1.2.10.2)

Table 15.4 *Required OIDs for collecting metrics on active connections*

Collecting data on new connections

You can use SNMP commands with various OIDs to gather and interpret data on the number of new connections on the BIG-IP system.

To gather and interpret the data for each of these metrics, you must perform some polling and calculations:

- First, *for each OID*, you must perform two separate polls, at a time interval of your choice.
- Next, you calculate the delta of the two poll values.
- Finally, *for each graph metric*, you perform a calculation on those OID deltas.

Table 15.5 shows the individual OIDS that you must poll to retrieve two separate poll values for each OID.

Performance Graph (Configuration utility)	Graph Metrics	Required SNMP OIDs
New Connections (summary graph)	Client Connects	sysStatClientTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.7)
	Client Accepts	sysTcpStatAccepts (.1.3.6.1.4.1.3375.2.1.1.2.12.6)
	Server Connects	sysTcpStatConnects (.1.3.6.1.4.1.3375.2.1.1.2.12.8)
Total New Connections (detailed graph)	Client Connects	sysStatClientTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.7)
	Server Connects	sysStatServerTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.14)
New PVA Connections (detailed graph)	pva client	sysStatPvaClientTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.21)
	pva server	sysStatPvaServerTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.28)
New Client SSL Profile Connections (detailed graph)	SSL Client	sysClientsslStatTotNativeConns (.1.3.6.1.4.1.3375.2.1.1.2.9.6) sysClientsslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.9.9)
	SSL Server	sysServersslStatTotNativeConns (.1.3.6.1.4.1.3375.2.1.1.2.10.6) sysServersslStatTotCompatConns (.1.3.6.1.4.1.3375.2.1.1.2.10.9)
New Accepts/Connects (detailed graph)	Client Accepts	sysTcpStatAccepts (.1.3.6.1.4.1.3375.2.1.1.2.12.6)
	Server Connects	sysTcpStatConnects (.1.3.6.1.4.1.3375.2.1.1.2.12.8)

Table 15.5 *Required OIDs for polling for data on new connections*

For example, for the **Client Accepts** graph metric:

1. Poll OID **sysTcpStatAccepts (.1.3.6.1.4.1.3375.2.1.1.2.12.6**) twice, at a 10-second interval.
   This results in two values, **<sysTcpStatAccepts1>** and **<sysTcpStatAccepts2>**.

Note: *Although this example uses an interval of ten seconds, the interval can actually be any duration that you choose.*

2. Calculate the delta of the two poll values:

```
<DeltaTcpStatAccepts> = <sysTcpStatAccepts2> - <sysTcpStatAccepts1>
```

3. Calculate the value of the **Client Accepts** graph metric using the calculation shown in Table 15.6 (**<DeltaTcpStatAccepts> / <interval>**), where the value of **<interval>** is **10**.

Performance Graph (Configuration utility)	Graph Metrics	Required calculations for new connection metrics
New Connections (summary graph)	Client Connections	<DeltaStatClientTotConns> / <interval>
	Client Accepts	<DeltaTcpStatAccept> / <interval>
	Server Connects	<DeltaTcpStatConnects> / <interval>
Total New Connections (detailed graph)	Client Connections	<DeltaStatClientTotConns> / <interval>
	Server Connections	<DeltaStatServerTotConns> / <interval>
New PVA Connections (detailed graph)	pva client	<DeltaStatPvaClientTotConns> / <interval>
	pva server	<DeltaStatPvaServerTotConns> / <interval>
New SSL Connections (detailed graph)	SSL Client	(<DeltaClientsslStatTotNativeConns> + <DeltaClientsslStatTotCompatConns>) / <interval>
	SSL Server	(<DeltaServersslStatTotNativeConns> + <DeltaServersslStatTotCompatConns>) / <interval>
New Accepts/Connects (detailed graph)	Client Accepts	<DeltaTcpStatAccepts> / <interval>
	Server Connects	<DeltaTcpStatConnects> / <interval>

Table 15.6 *Required calculations for interpreting metrics on new connections*

Collecting data on throughput rates

You can use SNMP commands with various OIDs to gather and interpret data on the throughput rate on the BIG-IP system, in terms of bits per second.

To gather and interpret the data for each of these metrics, you must perform some polling and calculations:

- First, *for each OID*, you must perform two separate polls, at an interval of your choice.
- Next, you calculate the delta of the two poll values.
- Finally, *for each graph metric*, you perform a calculation on those OID deltas.

Table 15.7 shows the individual OIDS that you must poll, retrieving two separate poll values for each OID.

Performance Graph (Configuration utility)	Graph Metrics	Required SNMP OIDs
Throughput (summary graph)	Client Bits	sysStatClientBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.3) sysStatClientBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.5)
	Server Bits	sysStatServerBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.10) sysStatServerBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.12)
Throughput (detailed graph)	Client Bits In	sysStatClientBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.3)
	Client Bits Out	sysStatClientBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.5)
	Server Bits In	sysStatServerBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.10)
	Server Bits Out	sysStatServerBytesOut (.1.3.6.1.4.1.3375.2.1.1.2.1.12)

Table 15.7 *Required OIDs for polling for data on throughput rates*

For example, for the **Server Bits In** graph metric:

1. Poll OID **sysStatServerBytesIn (.1.3.6.1.4.1.3375.2.1.1.2.1.10)** twice, at a 10-second interval.
   This results in two values, **<sysStatServerBytesIn1>** and **<sysStatServerBytesIn2>**.

   Note: *Although this example uses an interval of ten seconds, the interval can actually be any duration that you choose.*

2. Calculate the delta of the two poll values:

```
<DeltaStatServerBytesIn> = <sysStatServerBytesIn2> - <sysStatServerBytesIn1>
```

3. Calculate the value of the **Server Bits In** graph metric using the calculation shown in Table 15.8 (**<DeltaStatServerBytesIn> / <interval>**), where the value of **<interval>** is **10**.

Performance Graph (Configuration utility)	Graph Metrics	Required calculations for throughput rates
Throughput (summary graph)	Client Bits	((<DeltaStatClientBytesIn> + <DeltasysStatClientBytesOut>)*8) / <interval>
	Server Bits	((<DeltaStatServerBytesIn> + <DeltasysStatServerBytesOut>)*8) / <interval>

Table 15.8 *Required calculations for interpreting metrics on throughput rates*

Performance Graph (Configuration utility)	Graph Metrics	Required calculations for throughput rates
Throughput (detailed graph)	Client Bits In	(<DeltaStatClientBytesIn>*8) / <interval>
	Client Bits Out	(<DeltaStatClientBytesOut>*8) / <interval>
	Server Bits In	(<DeltaStatServerBytesIn>*8) / <interval>
	Server Bits Out	(<DeltaStatServerBytesOut>*8) / <interval>

Table 15.8 *Required calculations for interpreting metrics on throughput rates*

Collecting data on HTTP requests

You can use SNMP commands with an OID to gather and interpret data on the number of current HTTP requests on the BIG-IP system, in terms of requests per second.

To gather and interpret the data for this metric, you must perform some polling and calculations:

- First, you must use the OID to perform two separate polls, at an interval of your choice.
- Next, you calculate the delta of the two poll values.
- Finally, you perform a calculation on the OID delta.

Table 15.9 shows the OID that you must poll, retrieving two separate poll values for this OID.

Performance Graph (Configuration utility)	Graph Metric	Required SNMP OIDs
HTTP Requests	HTTP Requests	sysStatHttpRequests (.1.3.6.1.4.1.3375.2.1.1.2.1.56)

Table 15.9 *Required OIDs for polling for data on HTTP requests*

For example, for the **HTTP Requests** graph metric:

1. Poll OID **sysStatHttpRequests (.1.3.6.1.4.1.3375.2.1.1.2.1.56)** twice, at a 10-second interval.
   This results in two values, **<sysStatHttpRequests1>** and **<sysStatHttpRequests2>**.

   Note: *Although this example uses an interval of ten seconds, the interval can actually be any duration that you choose.*

2. Calculate the delta of the two poll values:

```
<DeltaStatHttpRequests> = <sysStatHttpRequests2> - <sysStatHttpRequests1>
```

3. Calculate the value of the **HTTP Requests** graph metric using the calculation shown in Table 15.10, where the value of **<interval>** is **10**.

Performance Graph (Configuration utility)	Graph Metric	Required calculations for HTTP requests
HTTP Requests	HTTP Requests	<DeltaStatHttpRequests> / <interval>

Table 15.10 *Required calculations for interpreting metrics on HTTP requests*

Collecting data on RAM Cache use

You can use an SNMP command with various OIDs to gather and interpret data on RAM cache use.

To gather and interpret the data for each of these metrics, you must perform some polling and calculations. First, *for each OID*, you must poll for data. Then, *for each graph metric*, you perform a calculation using the OID data.

Table 15.11 shows the individual OIDS that you must use to poll for Ram Cache data.

Performance Graph (Configuration utility)	Graph Metric	Required SNMP OID
RAM Cache Utilization	Hit Rate	sysHttpStatRamcacheHits (.1.3.6.1.4.1.3375.2.1.1.2.4.46) sysHttpStatRamcacheMisses (.1.3.6.1.4.1.3375.2.1.1.2.4.47)
	Byte Rate	sysHttpStatRamcacheHitBytes (.1.3.6.1.4.1.3375.2.1.1.2.4.49) sysHttpStatRamcacheMissBytes (.1.3.6.1.4.1.3375.2.1.1.2.4.50)
	Eviction Rate	sysHttpStatRamcacheEvictions (.1.3.6.1.4.1.3375.2.1.1.2.4.54) sysHttpStatRamcacheHits (.1.3.6.1.4.1.3375.2.1.1.2.4.46) sysHttpStatRamcacheMisses (.1.3.6.1.4.1.3375.2.1.1.2.4.47)

Table 15.11 *Required OIDs for polling for data on RAM Cache use*

For example, for the **Hit Rate** graph metric:

1. Poll the OID **sysHttpStatRamcacheHits (.1.3.6.1.4.1.3375.2.1.1.2.4.46).** This results in a value of **<sysHttpStatRamcacheHits1>**.
2. Poll the OID **sysHttpStatRamcacheMisses (.1.3.6.1.4.1.3375.2.1.1.2.4.47).** This results in a value of **<sysHttpStatRamcacheMisses1>**.

3. Calculate the value of the **Hit Rate** graph metric using the calculation shown in Table 15.12 (**<sysHttpStatRamcacheHits1> / (<sysHttpStatRamcacheHits1> + <sysHttpStatRamcacheMisses1>) *100**).

Performance Graph (Configuration utility)	Graph Metric	Required SNMP OID
RAM Cache Utilization	Hit Rate	<sysHttpStatRamcacheHits1> / (<sysHttpStatRamcacheHits1> + <sysHttpStatRamcacheMisses1>) *100
	Byte Rate	<sysHttpStatRamcacheHitBytes1> / (<sysHttpStatRamcacheHitBytes1> + <sysHttpStatRamcacheMissBytes1>) *100
	Eviction Rate	<sysHttpStatRamcacheEvictions1> / (<sysHttpStatRamcacheHits1> + <sysHttpStatRamcacheMisses1>) *100

Table 15.12 *Required calculations for interpreting metrics on RAM Cache use*

Collecting data on CPU use

You can use SNMP commands with various OIDs to gather and interpret data on CPU use on the BIG-IP system. Specifically, you can gather and interpret data for two different graph metrics: **TMM CPU Usage** and **CPU[0-n]**.

To gather and interpret the data for this metric, you must perform some polling and calculations:

- First, you must use the OID to perform two separate polls, at an interval of your choice.
- Next, you calculate the delta of the two poll values.
- Finally, you perform a calculation on the OID delta.

Table 15.13 shows the individual OIDS that you must poll, retrieving two separate poll values for each OID.

.

Performance Graph (Configuration utility)	Graph Metric	Required SNMP OIDs
CPU Usage	CPU[0-n]	sysHostCpuUser (.1.3.6.1.4.1.3375.2.1.7.2.2.1.3) sysHostCpuNice (.1.3.6.1.4.1.3375.2.1.7.2.2.1.4) sysHostCpuSystem (.1.3.6.1.4.1.3375.2.1.7.2.2.1.5) sysHostCpuUser (.1.3.6.1.4.1.3375.2.1.7.2.2.1.3) sysHostCpuNice (.1.3.6.1.4.1.3375.2.1.7.2.2.1.4) sysHostCpuIdle (.1.3.6.1.4.1.3375.2.1.7.2.2.1.5) sysHostCpuSystem (.1.3.6.1.4.1.3375.2.1.7.2.2.1.6) sysHostCpuIrq (.1.3.6.1.4.1.3375.2.1.7.2.2.1.7) sysHostCpuSoftirq (.1.3.6.1.4.1.3375.2.1.7.2.2.1.8) sysHostCpuIowait (.1.3.6.1.4.1.3375.2.1.7.2.2.1.9)
	TMM CPU Usage	sysStatTmTotalCycles (.1.3.6.1.4.1.3375.2.1.1.2.1.41) sysStatTmIdleCycles (.1.3.6.1.4.1.3375.2.1.1.2.1.42) sysStatTmSleepCycles (.1.3.6.1.4.1.3375.2.1.1.2.1.43)

Table 15.13 *Required OIDs for polling for data on CPU use*

For example, for the **CPU[0-n]** graph metric:

1. Poll the OID **sysHostCpuUser (.1.3.6.1.4.1.3375.2.1.7.2.2.1.3)** twice, at a 10-second interval.
   This results in two values, **<sysHostCpuUser1>** and **<sysHostCpuUser2>**.

   Note: *Although this example uses an interval of ten seconds, the interval can actually be any duration that you choose.*

2. Calculate the delta of the two poll values:

   ```
   <DeltaCpuUser = sysHostCpuUser2 - sysHostCpuUser1
   ```

3. Repeat steps one and two for each OID pertaining to the **CPU[0-n]** graph metric.

4. Calculate the value of the **CPU[0-n]** graph metric using the calculation shown in Table 15.14.

Performance Graph (Configuration utility)	Graph Metric	Required calculations for CPU use
CPU Usage	CPU[0-n]	(<DeltaCpuUser> + <DeltaCpuNice> + <DeltaCpuSystem>) / (<DeltaCpuUser> + <DeltaCpuNice> + <Delta CpuIdle> + <DeltaCpuSystem> + <DeltaCpuIrq> + <DeltaCpuSoftirq> + <DeltaCpuIowait>) *100
	TMM CPU Usage	((<DeltaTmTotalCycles> - (<DeltaTmIdleCycles> + <DeltaTmSleepCycles>)) / <DeltaTmTotalCycles>) *100

Table 15.14 *Required calculations for interpreting metrics on CPU use*

Collecting data on SSL transactions per second

You can use SNMP commands with an OID to gather and interpret data on SSL performance, in terms of transactions per second.

To gather and interpret the data for this metric, you must perform some polling and calculations:

- First, you must use the OID to perform two separate polls, at an interval of your choice.
- Next, you calculate the delta of the two poll values.
- Finally, you perform a calculation on the OID delta.

Table 15.15 shows the OID that you must poll, retrieving two separate poll values for this OID.

Performance Graph (Configuration utility)	Graph Metrics	Required SNMP OIDs
SSL TPS	SSL TPS	sysStatClientTotConns (.1.3.6.1.4.1.3375.2.1.1.2.1.7)

Table 15.15 *Required OIDs for polling for data on SSL TPS*

For example, for the **SSL TPS** graph metric:

1. Poll the OID **sysStatClientTotConns** (**.1.3.6.1.4.1.3375.2.1.1.2.1.7**) twice, at a 10-second interval.
   This results in two values, **<sysStatClientTotConns1>** and **<sysStatClientTotConns2>**.

   Note: *Although this example uses an interval of ten seconds, the interval can actually be any duration that you choose.*

2. Calculate the delta of the two poll values:

```
<DeltaStatClientTotConns> = <sysStatClientTotConns2> - <sysStatClientTotConns1>
```

3. Calculate the actual value of the **SSL TPS** graph metric using the calculation shown in Table 15.16, where the value of **<interval>** is **10**.

Performance Graph (Configuration utility)	Graph Metric	Required calculations for SSL TPS
SSL TPS	SSL TPS	<DeltaStatClientTotConns> / <interval>

Table 15.16 *Required calculations for interpreting metrics on SSL TPS*

16

Saving and Restoring Configuration Data

- Introducing archives
- Managing archives

Introducing archives

On any BIG-IP system, you have a set of data that you created when you initially configured the system, using the Setup utility and the Configuration utility. This data consists of traffic management elements such as virtual server definitions, pool definitions, and profiles. Configuration data also consists of system and network definitions such as interface properties, self IP addresses, VLAN configurations, redundant system settings, and more. Using the Archives feature, you can back up the current configuration data, and if necessary, restore the data at a later time. We highly recommend that you use this feature to mitigate the potential loss of BIG-IP system configuration data.

What is an archive?

Before you replace a version of the BIG-IP system with a newer version, you should always create an ***archive***, which is a backup copy of the configuration data. This archive is in the form of a ***user configuration set***, or UCS. Then, if you need to recover that data later, you can restore the data from the archive that you created.

A UCS contains the following types of BIG-IP system configuration data:

- System-specific configuration files
- Product licenses
- User accounts and password information
- Domain Name Service (DNS) zone files
- Installed SSL keys and certificates

Each time you back up the configuration data, the BIG-IP system creates a new file with a **.ucs** extension. Each UCS file contains various configuration files needed for the BIG-IP system to operate correctly, as well as the configuration data.

◆ **Note**

To create or restore an archive, you must have the ***Administrator*** *role assigned to your user account.*

Working with archives

Using the Configuration utility, you can save and restore archives that are stored on the BIG-IP system. Furthermore, for added security, you can save archives to and restore archives from a remote system, that is, the system on which you are running the Configuration utility.

Saving archives

On the BIG-IP system, the system stores all archives in the directory **/var/local/ucs**. When you create an archive, you cannot store the UCS file in a different directory. However, after you create the archive and it is stored in the **/var/local/ucs** directory, you can download a copy of the UCS file to the system from which you are running the Configuration utility (a remote system). This provides an extra level of protection by preserving the configuration data on a remote system. In the unlikely event that you need to restore the data, and a BIG-IP system event prevents you from accessing the archive in the **/var/local/ucs** directory, you still have a backup copy of the data.

◆ **Important**

*When creating an archive, you must assign a name to the archive file that matches the name of the BIG-IP system. For example, if you are creating an archive for a BIG-IP system named **bigip2**, the archive file must have the name **bigip2.ucs**.*

◆ **Important**

If your configuration data includes SSL keys and certificates, be sure to store the archive file in a secure environment.

Restoring archives

Not only is the **/var/local/ucs** directory the only location on the BIG-IP system in which you can save an archive, but it is also the only location on the BIG-IP system from which you can restore an archive. However, if you previously downloaded an archive to a remote system, and a BIG-IP system event prevents you from accessing the **/var/local/ucs** directory, you can upload the archive from that remote system.

Synchronizing data for redundant systems

When you have a redundant system configuration, it is essential that the same set of configuration data exists on both units of the BIG-IP system. To synchronize configuration data, you use the High Availability screens in the System area of the Configuration utility. To mitigate against data loss, however, you use the Archives screens.

We recommend that you use the Archives feature to routinely create an archive of the configuration data on each unit of the redundant system. Note, too, that when you synchronize configuration data for a redundant system, the BIG-IP system automatically creates a backup archive, named **cs_backup.ucs**, immediately prior to performing the synchronization. This ensures that you always have a copy of the most recent configuration data, in the event that a system event occurs during the synchronization process. For more information on synchronizing configuration data, see Chapter 13, *Setting up a Redundant System*.

Managing archives

As described in *Introducing archives*, on page 16-1, you can create, store, and access archives, on both the BIG-IP system and a remote system. You can also view any existing archive files and their properties, as well as delete archives that you no longer need. Specifically, you can use the Configuration utility to:

- View a list of existing archives
- Create a new archive and store it on the BIG-IP system
- View the properties of an existing archive
- Restore data from a BIG-IP system archive
- Download a copy of an archive to another system
- Upload a copy of an archive that you previously saved to another system
- Delete an existing archive from the BIG-IP system

Viewing a list of existing archives

You can view a list of archives (that is, UCS files) that are currently stored in the **/var/local/ucs** directory on the BIG-IP system. When you view a list of archives, the Configuration utility displays the following information:

- The name of the UCS file
- The date that the UCS file was created or uploaded
- The size of the file, in kilobytes

◆ **Note**

*Whenever you last upgraded the BIG-IP system to a new version, you were required to create a UCS file named **config.ucs**, using the **bigpipe config save** command. This UCS file appears in the list of UCS files on the Archives screen.*

To view a list of existing archives

On the Main tab of the navigation pane, expand **System**, and click **Archives**. The Archives screen opens, displaying a list of existing UCS files.

Creating and saving an archive on the BIG-IP system

You can create a new archive, which the BIG-IP system automatically stores in the directory **/var/local/ucs**. You can create as many separate archives as you want, as long as each archive has a unique file name. Note that the BIG-IP system cannot store the archive in any BIG-IP system directory other than **/var/local/ucs**. For more information on storing UCS files, see *Introducing archives*, on page 16-1.

When you create an archive, you configure some settings, such as a setting to encrypt the archive file for security reasons. Table 16.1 lists and describes these settings, and shows their default values.

Setting	Description	Default Value
File Name	Specifies the file name for the archive. You do not need to specify the UCS file name extension. The BIG-IP system appends the UCS extension automatically.	No default value
Encryption	Enables or disables encryption of the archive. If you select **Enabled**, two other settings, **Passphrase** and **Verify Passphrase**, appear on the screen.	**Disabled**
Passphrase	Specifies a password that a user must use to decrypt an archive.	No default value
Verify Passphrase	Specifies the password that you defined with the **Passphrase** setting.	No default value
Private Keys	Specifies whether to include or exclude private keys in the archive.	**Include**
Version	Displays the version of the BIG-IP system application that is currently running on the BIG-IP hardware platform. You cannot configure the **Version** setting.	No default value

Table 16.1 *Settings for creating an archive*

To create an archive

1. On the Main tab of the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the upper-right corner of the screen, click **Create.**
   The New Archive screen opens.
3. In the **File Name** box, type a unique file name for the archive.
   We recommend that the file name match the name of the BIG-IP system. For example, if the name of the BIG-IP system is **bigip2**, then the name of the archive file should be **bigip2.ucs**. For more information, see *Working with archives*, on page 16-1.
4. If you want to encrypt the archive, locate the **Encryption** list and select **Enabled**.

   Note: *If the* ***Encryption*** *setting is unavailable, you must configure the* ***Archive Encryption*** *setting located on the Preferences screen. For more information, see the description of the Configuration utility in Chapter 1,* ***Introducing BIG-IP Network and System Management****.*
5. If you want the BIG-IP system to include any private keys, locate the **Private Keys** list and select **Include**.
   In this case, be sure to store the archive file in a secure environment.
6. Click **Finished**.

Viewing archive properties

Using the Configuration utility, you can view the properties of an archive that you previously created. Note that you cannot modify the properties of an archive. If you want to modify an archive, you must delete the archive you want to change and then create a new one.

The properties of an archive that you can view are:

- The name of the archive
- The version of the BIG-IP system on which the archive was created
- The encryption state of the archive (encrypted or unencrypted)
- The date that the archive was created
- The size of the archive, in kilobytes

To view the properties of an archive

1. On the Main tab of the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the Name column, click the name of the archive that you want to view.
   This displays the properties of that archive.

Restoring data from a BIG-IP system archive

In the unlikely event that the BIG-IP system configuration data becomes corrupted, you can restore the data from the archive that is currently stored in the directory **/var/local/ucs**. If no archive exists in that directory, then you cannot restore configuration data.

◆ **Important**

The name of the archive must match the host name of the BIG-IP system you are restoring. For example, if the host name of the BIG-IP system you are restoring is ***bigip2****, then the name of the archive must be* ***bigip2.ucs****. If necessary, you can change the host name of the BIG-IP system to match the name of the archive.*

To restore data from a BIG-IP system archive

1. On the Main tab of the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the File Name column, click the name of the archive that you want to use to restore the configuration data.
   This displays the properties of that archive.
3. Click **Restore.**
   This restores the BIG-IP system configuration data.

Downloading an archive to a remote system

As described in the section *Introducing archives*, on page 16-1, you can download a copy of an existing archive to a remote system, that is, the system from which you ran the Configuration utility to create the archive. This feature protects the configuration data in the unlikely event that the BIG-IP system experiences a system catastrophe.

When you download an existing archive, you first display the properties of the archive you want to download, and then specify the complete path name of the location to which you want to save the archive copy.

To download an archive

1. On the Main tab of the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the File Name column, click the name of the archive that you want to view.
   This displays the properties of that archive.
3. For the **Archive File** setting, click the **Download: <.ucs filename>** button.
   A confirmation screen appears.
4. Click **Save**.
   The BIG-IP system downloads a copy of the UCS file to the system from which you initiated the download.

Uploading an archive from a remote system

If you previously downloaded a copy of an archive to a remote system (that is, the system from which you initiated the download), you can upload that archive to the BIG-IP system at any time. This is most useful when a BIG-IP system event has occurred that has caused the archive stored on the BIG-IP system to either become unavailable or corrupted for some reason.

Note that when you upload a copy of an archive, you must specify the exact path name for the directory in which the downloaded archive copy is stored.

To upload an archive

1. On the Main tab of the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the upper-right corner of the screen, click **Upload**.
   This opens the Upload screen.
3. In the **File Name** box, type the complete path and file name of the archive that you want to upload onto the BIG-IP system.
   If you do not recall the path or file name, you can use the **Browse** button to locate and select the file name.

4. For the **Options** setting, check the **Overwrite existing archive file** box if you want the BIG-IP system to overwrite any existing archive file.

   Note: *The BIG-IP system overwrites an existing file with the uploaded file only when the name of the archive you are uploading matches the name of an archive on the BIG-IP system.*

5. Click **Upload**.
   This uploads the specified archive to the directory **/var/local/ucs** on the BIG-IP system.

Deleting an archive

You can use the Configuration utility to delete any archive on the BIG-IP system that is stored in the directory **/var/local/ucs.**

To delete an archive

1. On the Main tab of the navigation pane, expand **System**, and click **Archives**.
   The Archives screen opens.
2. In the File Name column, locate the name of the archive you want to delete.
3. To the left of the archive name, check the Select box.
4. Click **Delete**.
   A confirmation box appears.
5. Click **Delete** again.
   This deletes the archive from the **/var/local/ucs** directory on the BIG-IP system.

17

Logging BIG-IP System Events

- Introducing BIG-IP system logging
- Understanding log types
- Setting log levels
- Configuring encrypted remote logging

Introducing BIG-IP system logging

Viewing and managing log messages is an important part of maintaining a BIG-IP system. Log messages inform you on a regular basis of the events that are happening on the system. Some of these events pertain to general events happening within the operating system, while other events are specific to the BIG-IP system, such as the stopping and starting of BIG-IP system services.

The mechanism that the BIG-IP system uses to log events is the Linux utility **syslog-ng**. The ***syslog-ng*** utility is an enhanced version of the standard UNIX and Linux logging utility **syslog**.

The types of events that the BIG-IP system logs are:

- **System events**
  System event messages are based on Linux events, and are not specific to the BIG-IP system.

- **Packet filter events**
  Packet filter messages are those that result from the implementation of packet filters and packet-filter rules.

- **Local traffic events**
  Local-traffic event messages pertain specifically to the local traffic management system.

- **Audit events**
  Audit event messages are those that the BIG-IP system logs as a result of changes to the BIG-IP system configuration. Logging audit events is optional.

Summarizing logging features

The logging mechanism on a BIG-IP system includes several features designed to keep you informed of system events in the most effective way possible.

One of the primary features of the logging feature is its ability to log different types of events, ranging from Linux system events, to packet filtering events, to local traffic events. Through the BIG-IP system auditing feature, you can even track and report changes that users make to the BIG-IP system configuration, such as adding a virtual server or designating a device to be part of a redundant system. For more information, see *Understanding log content*, on page 17-2 and *Understanding log types*, on page 17-4.

When setting up logging on the BIG-IP system, you can customize the logs by designating the minimum severity level, or log level, that you want the BIG-IP system to report when a type of event occurs. The ***minimum log level*** indicates the minimum severity level at which the BIG-IP system logs that type of event.

For example, you can specify that, for any change a user makes to the bigdb^{TM} database, the minimum severity level for which the BIG-IP system logs messages is **Warning**. This means that the BIG-IP system logs **Warning** and more severe messages such as **Error** and **Critical** messages, but not less severe ones such as **Notice**, **Informational**, or **Debug** messages. For more information, see *Setting log levels*, on page 17-7.

You can also use the Configuration utility to search for a string within a log event, that is, filter the display of the log messages according to the string you provide. For more information, see *Viewing and filtering log messages*, on page 17-3.

Finally, you can log BIG-IP system events to a remote logging server. You do this by identifying the IP address or host name of the remote logging server, and creating an encrypted network connection, or tunnel, for sending log information to that remote server. For more information, see *Configuring encrypted remote logging*, on page 17-10.

◆ **Tip**

You can also configure the system to send email or activate pager notification based on the priority of the logged event.

Understanding log content

The logs that the BIG-IP system generates include several types of information. For example, all logs except the audit log show a timestamp, host name, and service for each event. Some logs show a status code, while the audit log shows a user name and a transaction ID corresponding to each configuration change. All logs contain a 1-line description of each event.

Table 17.1 lists the categories of information contained in the logs and the specific logs in which the information is displayed.

Information Type	Explanation	Log Type
Timestamp	The time and date that the system logged the event message.	System Packet Filter Local Traffic
Host name	The host name of the system that logged the event message. Because this is typically the host name of the local machine, the appearance of a remote host name could be of interest.	System Packet Filter Local Traffic
Service	The service that generated the event.	System Packet Filter Local Traffic
Status code	The status code associated with the event. Note that only events logged by BIG-IP system components, and not Linux system services, have status codes.	Packet Filter Local Traffic

Table 17.1 *Log information categories and their descriptions*

Information Type	Explanation	Log Type
Description	The description of the event that caused the system to log the message.	System Packet Filter Local Traffic
User Name	The name of the user who made the configuration change.	Audit
Transaction	The identification number of the configuration change.	Audit
Event	A description of the configuration change that caused the system to log the message.	Audit

Table 17.1 *Log information categories and their descriptions*

Viewing and filtering log messages

Use the Configuration utility for an easy way to view the log files that the system generates. You can also control which messages the Configuration utility displays, by typing a search string.

To view log messages

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   The Logs screen opens.
2. On the menu bar, click **System**, **Packet Filter**, **Local Traffic**, or **Audit**, depending on the type of log messages you want to view.
   This displays a list of this type of log message.
3. If you want to advance to another screen of messages, first locate the page list at the lower-right corner of the screen. You can either:
   - Display the list and select a page number or **Show All**.
   - Click the right arrow to advance to the next page of messages.

To filter log messages based on a search string

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   The Logs screen opens.
2. On the menu bar, click **System**, **Packet Filter**, **Local Traffic**, or **Audit**, depending on the type of log messages you want to view.
   This displays log messages of the type you selected.
3. In the Search box (directly above the Timestamp column), type a string, optionally using the asterisk as a wildcard character.
4. Click **Search**.
   This displays only those messages containing the string you specified.

Understanding log types

As described in *Introducing BIG-IP system logging*, on page 17-1, the BIG-IP system automatically logs four main event types: system, packet filter, local traffic, and configuration changes (audit). Each type of event is stored in a separate log file, and the information stored in each log file varies depending on the event type. All log files for these event types are in the directory **/var/log**.

Logging system events

Many events that occur on the BIG-IP system are Linux-related events, and do not specifically apply to the BIG-IP system. The BIG-IP system logs the messages for these events in the file **/var/log/messages**.

Using the Configuration utility, you can display these system messages. Table 17.2 shows some sample system log entries.

Timestamp	Host	Service	Event
Mon Feb 14 03:34:45 PST 2005	bigip3	syslog-ng[5494]	new configuration initialized
Mon Feb 14 03:35:06 PST 2005	bigip3	syslog-ng[5494]	kjournald starting. Commit interval 5 seconds.
Mon Feb 14 04:38:06 PST 2005	bigip3	EXT3-fs	mounted filesystem with ordered data mode.

Table 17.2 *Sample system log entries*

Logging packet filter events

Some of the events that the BIG-IP system logs are related to packet filtering. The system logs the messages for these events in the file **/var/log/pktfilter**.

Using the Configuration utility, you can display these packet filter messages.

Logging local traffic events

Many of the events that the BIG-IP system logs are related to local area traffic passing through the BIG-IP system. The BIG-IP system logs the messages for these events in the file **/var/log/ltm**.

Using the Configuration utility, you can display these local-traffic messages. Table 17.3 shows some sample local-traffic log entries.

Timestamp	Host	Service	Status Code	Event
Mon Feb 14 03:34:45 PST 2005	bigip2	bcm56xxd(785)	00010013	Starting packet registry event timer
Mon Feb 14 03:35:06 PST 2005	bigip2	bcm56xxd(785)	00010013	Starting HA heartbeat timer tick
Mon Feb 14 04:38:06 PST 2005	bigip2	bcm56xxd(785)	00010013	Successful start. Entering main message loop
Mon Feb 14 o4:36:06 PST 2005	bigip2	bcm56xxd(785)	00010012	Link 2.5 is up

Table 17.3 *Sample local-traffic log entries*

Some of the specific types of events that the BIG-IP system displays on the Local Traffic logging screen are:

- Address Resolution Protocol (ARP) packet and ARP cache events
- bigdb™ database events (such as populating and persisting bigdb variables)
- HTTP protocol events
- HTTP compression events
- IP packet discard events due to exceptional circumstances or invalid parameters (such as a bad checksum)
- Layer 4 events (events related to TCP, UDP, and Fast L4 processing)
- MCP/TMM configuration events
- Monitor configuration events
- Network events (layers 1 and 2)
- Packet Velocity® ASIC (PVA) configuration events
- iRule™ events related to run-time iRule processing
- SSL traffic processing events
- General TMM events such as TMM startup and shutdown

◆ **Note**

*For information on setting a minimum log level on each of these event types, see **Setting log levels for local traffic events**, on page 17-7, and Appendix B, **Configuring bigdb Database Keys**.*

Auditing configuration changes

Audit logging is an optional feature that logs messages whenever a BIG-IP system object, such as a virtual server or a load balancing pool, is configured; that is, created, modified, or deleted. There are three ways that objects can be configured:

- By user action
- By system action
- By loading configuration data

The BIG-IP system logs the messages for these events in the file **/var/log/ltm**.

Using the Configuration utility, you can display audit log messages. Table 17.4 shows some sample audit log entries. In this example, the first entry shows that user Janet enabled the audit logging feature, while the second and third entries show that user Matt designated the BIG-IP system to be a redundant system with a unit ID of **1**.

Timestamp	User Name	Transaction	Event
Mon Feb 14 03:34:45 PST 2005	janet	79255-1	DB_VARIABLE modified: name="config.auditing"

Mon Feb 14 03:35:06 PST 2005	matt	79609-1	DB_VARIABLE modified:
			name="failover.isredundant"
			value="true"

Mon Feb 14 03:35:06 PST 2005	matt	79617-1	DB_VARIABLE modified:
			name="failover.unitid"
			value="1"

Table 17.4 *Sample audit log entries*

By default, audit logging is disabled. For information on enabling this feature, see *Setting log levels*, following.

Setting log levels

Using the Configuration utility, you can set log levels on both local traffic and auditing events. For each type of local traffic event, you can set a minimum log level. The ***minimum log level*** indicates the minimum severity level at which the BIG-IP system logs that type of event. For more information, see *Setting log levels for local traffic events*, following.

For auditing events, you can set a log level that indicates the type of event that the system logs, such as the user-initiated loading of BIG-IP system configurations, or system-initiated configuration changes. For more information, see *Setting log levels for auditing events*, on page 17-9.

Setting log levels for local traffic events

For local traffic events, you can set a minimum log level. Thus, for different kinds of local traffic events, such as bigdb configuration events or events related to HTTP compression, you can set different minimum log levels.

The log levels that you can set on certain types of events, ordered from highest severity to lowest severity, are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

For example, if you set the minimum log level for bigdb events to **Error**, then the system only logs messages that have a severity of **Error** or higher for those events. If you retain the default minimum log level (**Informational**), then the system logs all messages that have a severity of **Informational** or higher (that is, all messages except **Debug** messages).

There are many different types of local traffic events for which you can set a minimum log level. Table 17.5 shows the types of local traffic events and the minimum log levels that you can configure for them. Because not all log levels are available for every local-traffic event type, the table shows the specific log levels you can set on each event type. Following the table is the procedure for setting the minimum log level on a local traffic event type.

Local-Traffic Event Type	Available Minimum Log Levels	Default Value
ARP/NDP	Error, Warning, Notice, Informational, Debug	Warning
BigDB	Critical, Error, Warning, Notice, Informational, Debug	Informational
HTTP	Error, Debug	Error
HTTP Compression	Error, Debug	Error
IP	Warning, Notice	Notice
iRules	Error, Informational, Debug	Informational
Layer 4	Notice, Informational, Debug	Notice
MCP	Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug	Notice
Monitors	Error, Debug	Error
Network	Critical, Error, Warning, Notice, Informational, Debug	Warning
Packet Velocity® ASIC	Informational, Debug	Informational
SSL	Error, Warning	Warning
Traffic Management OS	Emergency, Critical, Error, Notice, Informational	Error

Table 17.5 *Local-traffic event types and their available log levels*

To set a minimum log level for local traffic events

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   This opens the Logs screen.
2. On the menu bar, click **Options**.
   This displays the screen for setting minimum log levels on local traffic events.
3. In the Local Traffic Logging area of the screen, locate the event type for which you want to set a minimum log level.
   An example of an event type is HTTP Compression.

4. Select a minimum log level from the list.
5. Click **Update**.

◆ **Note**

For more information on local traffic event types, see ***Logging local traffic events****, on page 17-4. For information on using bigdb configuration keys to set minimum log levels, see Appendix B,* ***Configuring bigdb Database Keys****.*

Setting log levels for auditing events

An optional type of logging that you can enable is audit logging. Audit logging logs messages that pertain to configuration changes that users or services make to the BIG-IP system configuration. (For more information, see *Auditing configuration changes*, on page 17-6.)

You can choose one of four log levels for audit logging. In this case, the log levels do not affect the severity of the log messages; instead, they affect the initiator of the audit event.

The log levels for audit logging are:

- **Disable**
  This turns audit logging off. This is the default value.
- **Enable**
  This causes the system to log messages for user-initiated configuration changes only.
- **Verbose**
  This causes the system to log messages for user-initiated configuration changes and any loading of configuration data.
- **Debug**
  This causes the system to log messages for all user-initiated and system-initiated configuration changes.

To set a minimum log level for audit events

1. On the Main tab of the navigation pane, expand **System**, and click **Logs**.
   This opens the Logs screen.
2. On the menu bar, click **Options**.
   This displays the screen for setting minimum log levels on local traffic events.
3. In the Audit Logging area of the screen, select a log level from the **Audit** list.
4. Click **Update**.

Configuring encrypted remote logging

You can configure the Syslog utility on the BIG-IP system to send BIG-IP system log information to a remote logging host, using an encrypted network connection. To do this, you create a port-forwarding SSH tunnel to the remote logging host, and configure **syslog-ng** on the BIG-IP system to send log messages through the SSH tunnel.

Before you begin

Before you attempt to configure encrypted remote logging, you must meet the following conditions on the BIG-IP system and your remote logging host:

- **On the BIG-IP system**
  You must have a console with root access to the BIG-IP system.
- **On the remote logging host**
  You must have a console with root access to the remote logging host, the IP address, or the host name of the remote logging host.
- **For both systems**
  You must have both systems connected to the same subnetwork.

◆ **WARNING**

You should attempt this configuration only if you understand the risks associated with making changes to service startup scripts.

Creating the remote encrypted logging configuration

When creating an encrypted remote logging configuration, you must complete the following tasks:

- Review the SSH syntax required to create this configuration.
- Create a unique SSH identity key to identify and authorize the BIG-IP system.
- Edit the **syslog-ng** service startup script to create and destroy the SSH tunnels.
- Edit the remote logging host to accept **syslog-ng** messages through the SSH tunnel.
- Copy the unique SSH identity key to the remote logging host and append it to the authorized key file.
- Verify the logging configuration and restart **syslog-ng**.

Reviewing the SSH syntax required to create this configuration

This configuration requires that the BIG-IP system is able to establish an SSH connection to the remote logging host. On the BIG-IP system, use the **ssh** command to create the tunnel. Figure 17.1 is an example of the syntax required to create an SSH tunnel.

```
$ ssh -L <local tunnel port>:<remote log hostname>:<remote
tunnel port> \
  <remote user>@<remote log hostname> \
  -nNCxf \
  -i <key identity file>
```

Figure 17.1 *Establish an SSH tunnel from the BIG-IP system to the logging host.*

Table 17.6 contains detailed descriptions of the **ssh** syntax elements shown in Figure 17.1.

SSH syntax	Description
<local tunnel port>	The port SSH listens on for connections in order to forward them to **<remote log hostname>:<remote tunnel port>**.
<remote log hostname>	The IP address or FQDN of the remote logging server.
<remote tunnel port>	The port to which you want the SSH daemon on the remote logging server to forward connections.
<remote user>	The user name that **ssh** attempts to authenticate, as on **<remote log hostname>**.
<key identity file>	A file name from which the identity (private key) for authentication is read.

Table 17.6 *Detailed syntax elements for configuring SSH.*

Creating a unique SSH key to identify and authorize the BIG-IP system

After you have reviewed the **ssh** command syntax, use the **ssh** command to create the encrypted tunnel on the BIG-IP system, you must create a unique key on the BIG-IP system. The unique key is used to identify and authorize the BIG-IP system to the remote logging host.

Use the following command to create the file **syslog_tunnel_ID** and **syslog_tunnel_ID.pub**.

```
$ ssh -b 2048 -f syslog_tunnel_ID -t rsa -N "" -P ""
```

Use the following command to make **syslog_tunnel_ID** readable only by the **root** account:

```
$ chmod 600 syslog_tunnel_ID
```

Use the following command to make the public portion of the unique SSH ID named **syslog_tunnel_ID.pub** readable by all accounts:

```
$ chmod 644 syslog_tunnel_ID.pub
```

Copy **syslog_tunnel_ID** and **syslog_tunnel_ID.pub** into **/var/ssh** with the following command:

```
$ cp syslog_tunnel_ID* /var/ssh
```

Editing the syslog-ng start script to open and close the encrypted tunnel

Next change the **syslog-ng** start script, **/etc/init.d/syslog-ng**, so that the encrypted tunnel is opened when the **syslog-ng** script starts up and is closed when the script is restarted or stopped.

Before you edit the **syslog-ng** start script, save a backup copy to the root directory. Use the following command to save the backup to the root directory:

```
$ cp /etc/init.d/syslog-ng /root/syslog-ng.backup
```

After you save a backup of the **syslog-ng**, edit the startup script **/etc/init.d/syslog-ng** to automatically create a SSH tunnels when **syslog-ng** is started, or closed when **syslog-ng** is restarted or stopped.

The example configuration in this document demonstrates how to create a tunnel to a host using the following IP addresses and ports:

- IP address of **10.0.0.100**
- Local tunnel port of **5140**
- Remote tunnel port of **5140**
- User name **logger** on host **10.0.0.100**.

Start by adding syntax below the line that reads **start**). Figure 17.2 is an example of what the section of the **syslog-ng** start script looks like after you add the new syntax. In this example, the syntax you need to add is shown with bold text).

```
start)
      ssh -L 5140:10.0.0.100:5140 \
      logger@10.0.0.100 -nNCxf \
      -i var/ssh/syslog_tunnel_ID
       echo -n "Starting $INIT_NAME: "
       daemon --check $INIT_PROG "$INIT_PROG $INIT_OPTS"
```

Figure 17.2 *The syntax to add below the start) line.*

Next, add syntax below the line that reads **stop)**. Figure 17.3 shows the syntax you need to add in bold text.

```
stop)
       for sshTunnel in \
          `ps -ewo "%p!%a" | \
           grep ssh | \
           grep syslog_tunnel_ID | \
           grep -v grep | \
           cut -f 1 -d !`; do
           if [ -n "$sshTunnel" -a $sshTunnel -gt 10 ]; then
               echo " -- Shutting down SSH tunnel with process $sshTunnel"
               kill -TERM $sshTunnel
           fi
       done
       echo -n "Stopping $INIT_NAME: "
```

Figure 17.3 *The syntax to add below the stop) line*

Editing syslog-ng to log messages on the remote logging host

After you add the syntax to open and close SSH tunnels, you can edit the **syslog-ng** configuration to log messages to the remote machine. To do this, you need to create source and filter configuration blocks based on the local environment.

Using the example IP addresses and ports used in the example in the previous section, you would edit the **syslog-ng.conf** file to look like the **syslog-ng.conf** in Figure 17.4.

```
# capture all messages
filter f_catchall {
   level(debug...emerg);
};

# send message to localhost through tcp port 5140
destination d_remoteLogTunnel {
   tcp("127.0.0.1" port(5140););
};

# Combine everything to actually perform logging
log {
   source(local);
   filter(f_catchall);
   destination(d_remoteLogTunnel);
};
```

Figure 17.4 *The* ***syslog-ng.conf*** *example configuration*

Copying the unique SSH identity to the remote logging host and appending it to the authorized keys file

After you have edited the **syslog-ng.conf** to log messages on the remote logging host, you must copy the unique SSH identity to the remote logging host. To do this, copy the **syslog_tunnel_ID.pub** to the remote syslog server, and append this key to the **authorized_keys** file found in the**.ssh** folder under the home directory of the user that you want to use to capture remote log messages.

```
$ cat syslog_tunnel_ID.pub >> ~logger/.ssh/authorized_keys
```

Note

The following instructions are given as examples. The actual process for setting up the new SSH key to be automatically authorized, and configuring the syslog service may be different.

Verify that the logging facility is configured and ready to receive syslog messages on the **<remote tunnel port>**. If the remote logging host uses **syslog-ng**, you need to add a source configuration block like the one in Figure 17.5:

```
source remote {
   tcp(ip(10.0.0.100) port(5140));
};
```

Figure 17.5 *Remote logging host source identification block.*

In addition to the source identification block, you also need to add filter, destination, and log configuration blocks to use the data from the source **remote** as required by your application.

Verifying the logging configuration and restarting syslog-ng

Finally, verify that the SSH connection is functional and restart the **syslog-ng** service.

To verify the configuration from a command line and restart the syslog-ng service

1. Log in as **root** to the BIG-IP system.
2. Make an SSH connection to the remote logging host using the new identity key you created.

   ```
   # ssh logger@10.0.0.100 -i /var/shh/syslog_tunnel_ID
   ```

   If everything is configured correctly, you should be able to get shell access to the remote logging host without being challenged for a password. (By adding the new identity key to the remote host's **authorized_keys** file, the key is used to authenticate the BIG-IP system.)

3. Exit from the SSH session to the BIG-IP system command line.
4. Restart the **syslog-ng** service by typing the following command:

   ```
   $ /etc/init.d/syslog-ng restart
   ```

   The BIG-IP system should now be sending log messages to your remote host.

18

Configuring BIG-IP System Services

- Introducing BIG-IP System Services
- Managing core services
- Managing optional services

Introducing BIG-IP System Services

The BIG-IP system includes several services that you can start or stop. Also known as daemons, ***services*** perform a variety of functions, such as handling messaging and configuration data, managing application traffic, and monitoring the health and performance of load balancing servers.

Services also log events. Thus, within the Configuration utility, some of the logging screens display, for each message, the service that reported the event. The logging screens that show service names are the System screen, the Packet Filters screen, and the Local Traffic screen.

You can think of services as belonging to two categories: ***core services***, which start up when you boot the BIG-IP system and run continually, and ***optional services***, which are not essential for basic operation. The tasks required to manage all of these services differ depending on whether the service is a core service or an optional service.

◆ **Important**

You must have an ***Administrator*** *user role assigned to your user account to stop, start, or restart a service.*

Managing core services

The BIG-IP system starts a number of services at boot time, and they remain running as long as the BIG-IP system is operational. Most of these services are essential to the basic operation of the system.

Summarizing the core services

A number of system services start up automatically when you boot the BIG-IP system. Table 18.1 lists the BIG-IP system services that start up at boot time, and indicates the impact to BIG-IP system operation if the service is not running:

Service	Description	Impact When Unavailable
alertd	Monitors error messages and triggers proper action.	Cannot send alerts to front panel; cannot send SNMP traps; cannot monitor and handle error messages.
BCMX56XXD	Controls the BIG-IP switch hardware.	Cannot process switch traffic; LEDs, Link Aggregation Control Protocol (LACP) and spanning tree protocols (STP) cannot function..
BIGD	Controls health monitoring.	Cannot monitor health or performance of network devices.
bigdb	Provides initial BIgDB^{TM} database values to the MCPD service and persists any database changes to the **BigDB.dat** file.	Cannot initialize MCPD service; cannot load or save BigDB^{TM} database values.
chmand	Provides chassis monitoring and configuration, as well as other related functions.	Cannot perform platform identification, send platform information to MCPD service, or start SCCP services.
crond	Runs scheduled commands.	Cannot run daily or weekly scripts.
cssd	Performs configuration synchronization for redundant systems.	Cannot perform configuration synchronization.
fpdd	Handles front-panel display functions.	Cannot provide front panel data.
httpd	Provides HTTP web server functions.	Cannot provide Configuration utility or iControl.
lacpd	Creates trunks based on the industry-standard Link Aggregation Control Protocol (LACP) and controls the Switchboard Fail-safe feature for redundant systems.	Cannot aggregate links.
MCPD	Known as the Master Control Program, controls messaging and configuration.	Cannot manage traffic; cannot retrieve or update system status; users cannot reconfigure system; disables some of the other services.

Table 18.1 *Core system services*

Service	Description	Impact When Unavailable
snmpd	Provides System Network Management Protocol (SNMP) functions. Also includes the two subagents **rmondsnmpd** and **tmsnmpd**.	Cannot perform SNMP functions.
SOD	Controls failover for redundant systems.	Removes failover capability.
sshd	Provides remote access to the BIG-IP system command line interface.	Cannot provide remote access to the command line interface.
stpd	Implements the IEEE spanning tree protocols for preventing bridging loops.	Cannot detect bridging loops.
syslogd	Performs system logging based on the **syslog-ng** utility.	Cannot generate system logs.
tamd	Provides remote authentication and authorization.	Cannot perform remote authentication/authorization.
TMM	Known as the Traffic Management Microkernel, manages switch traffic.	Cannot process user application traffic or any UDP traffic.

Table 18.1 *Core system services*

Starting and stopping core services

In almost no case do you ever need to explicitly stop a core service from running. (The TMM service is a notable exception.) For this reason, you cannot use the Configuration utility to start or stop a core service. If you want to explicitly stop or start a core service, you use the **bigstart** command line utility. For information on the **bigstart** utility, see the **bigstart** man page. For information on stopping the TMM service, see *Traffic Management Microkernel service*, on page 18-4.

Configuring core services to control failover

System services have heartbeats. A service ***heartbeat*** is a recurring signal that a service generates. The BIG-IP system continually monitors service heartbeats to determine whether the service is still running. For some services, if the system does not detect a heartbeat, the system takes some action with respect to failover. These services are:

- MCPD
- TMM
- SOD
- BIGD
- BCMX56XXD

You can use the Configuration utility to control the way that the BIG-IP system behaves with respect to failover when the system no longer detects the heartbeat of these services. For example, you can configure the MCP service so that if its heartbeat is undetected, the BIG-IP system automatically fails over to the peer unit. For more information, see Chapter 13, *Setting up a Redundant System*.

Understanding the MCPD, TMM, and SOD services

The core services MCPD, TMM, and SOD are important because they support key functions of the BIG-IP system. These services run automatically unless you specifically shut them down. They provide essential functions such as maintaining the BIG-IP system configuration data, passing application traffic through TMM switch interfaces, and performing failover for redundant system configurations.

The Master Configuration Process service

The ***Master Configuration Process*** service (MCPD) manages the configurations on a BIG-IP system. The primary purpose of the MCPD service is to:

- Receive and process configuration change requests from MCP clients, validate configuration change requests based on database schema and other complex BIG-IP system business rules, and update storage for the target configuration. The service also returns success or failure results to clients.
- Receive and process statistics and configuration query requests from MCP clients and return query results to the clients.
- Support a publish-and-subscribe interface, where the service can notify all interested MCP clients of any configuration changes that might be of interest to those clients.

Traffic Management Microkernel service

The Traffic Management Microkernel (TMM) service is the process running on the BIG-IP system that performs most traffic management for the product. As such, the TMM service supports all system and networking components that the BIG-IP system needs in order to process application and administrative traffic. The TMM service controls all system interfaces, except for the management interface (**MGMT**).

A separate instance of the TMM service runs for each active processor on the BIG-IP system.

The TMM service affects the type of interface (TMM switch interface or management interface) that the BIG-IP system uses for network traffic. The effect on the use of BIG-IP interfaces differs depending on the type of traffic. Normally, when the TMM service is running, certain types of network traffic use the management interface, while other types of traffic use the TMM switch interfaces:

- **User application traffic**
  This type of traffic is typically application traffic either destined for or coming from a load balancing server or other network device. User application traffic always uses TMM switch interfaces, and never uses the management interface. Therefore, if the TMM service is stopped, the BIG-IP system does not process this type of traffic.

- **Administrative traffic destined for the BIG-IP system**
  This type of traffic is traffic destined for the IP address of the BIG-IP system's management interface. The BIG-IP system then sends its responses to these requests back through the management interface. (The exception to this is UDP traffic, which the BIG-IP system sends out using the TMM default route.) Because administrative traffic uses the management interface, the BIG-IP system can still process this type of traffic when the TMM service is not running.

- **Administrative traffic coming from the BIG-IP system**
  The BIG-IP system generates this type of administrative traffic, and the source for this type of traffic is the IP address of the management interface. When the TMM service is running, the BIG-IP system sends this type of traffic through a TMM switch interface, using the TMM default route. If the TMM service becomes unavailable, this type of traffic uses the management interface.

◆ **WARNING**

When the TMM service is running, make sure that you have defined a default route in the main TMM routing table. Defining a TMM default route prevents high volumes of administrative traffic generated by the BIG-IP system from using the management interface. For more information, see Chapter 8, ***Configuring Routes****.*

To summarize, Figure 18.2 lists the three main traffic types, and shows the type of BIG-IP system interface that each traffic type uses when the TMM service is running:

Traffic Type	Incoming Interface	Outgoing Interface
User application traffic	TMM	TMM
Administrative traffic destined for management interface IP address	MGMT	MGMT (for non-UDP traffic) TMM (for UDP traffic, when TMM default route is defined)
Administrative traffic that the BIG-IP system generates	Not Applicable	TMM (when TMM default route is defined) ***Note:*** *See note following this table.*

Table 18.2 *BIG-IP interfaces used when TMM is running*

◆ **Note**

Traffic generated by the nptd service in particular does not normally use a TMM interface when the TMM is running. Instead, the service uses the MGMT interface. The only case in which the ntpd service uses a TMM interface is when the ntpd service has been restarted for some reason. In this case, the service switches from using the MGMT interface to using a TMM interface. For more information on the ntpd service, see Chapter 4, ***Configuring the BIG-IP Platform and General Properties****.*

There are certain administrative tasks, however, such as a BIG-IP software installation, that you should never perform while the TMM service is running. Prior to performing these tasks, you should shut down the TMM service.

When you stop the TMM service and therefore make the TMM interfaces unavailable, the management interface becomes the only available interface on the BIG-IP system for administrative traffic. Figure 18.3 shows the type of interface that each traffic type uses when the TMM is stopped.

Traffic Type	Incoming Interface	Outgoing Interface
User application traffic	None available	None available
Administrative traffic destined for management interface IP address	MGMT	MGMT
Administrative traffic that the BIG-IP system generates	Not Applicable	MGMT

Table 18.3 *BIG-IP interfaces used when TMM is stopped*

◆ **Important**

The BIG-IP system drops UDP packets when the TMM service is running but no TMM default route is defined.

Other administrative tasks that you should perform using the management interface only (because they require you to stop the TMM service) are a PXE installation and boot, and remote management using SSH and HTTPS.

◆ **Note**

The BIG-IP system normally routes remote authentication traffic through a Traffic Management Microkernel (TMM) switch interface (that is, an interface associated with a VLAN and a self IP address), rather than through the management interface. Therefore, if the TMM service has been stopped for any reason, remote authentication is not available until the service is running again. For information on configuring remote authentication of application traffic, see the ***Configuration Guide for Local Traffic Management****.*

SOD service

The SOD service runs on a unit of a redundant system and monitors the peer unit. If the redundant system is an active/standby configuration, the SOD service runs on the standby unit and monitors the active unit. If the redundant system is an active-active configuration, the SOD service runs on both units, and each SOD service monitors the peer unit. When the SOD service determines that the peer unit is no longer responding, the service initiates failover.

The SOD service can monitor the active unit in two ways, either through a serial line (known as ***hardwired failover***) or through the network (known as ***network failover***). The default configuration for the SOD service is to perform hardwired failover.

To summarize, the primary purpose of the SOD service is to:

- Monitor and communicate with the peer unit of a redundant system
- Scan for requests by other processes for the SOD service to initiate a failover
- Initiate failover

For more information on managing a redundant system, see Chapter 13, *Setting up a Redundant System*, and Appendix B, *Configuring bigdb Database Keys*.

Managing optional services

The BIG-IP system includes a number of services that you can start, stop, or restart using the Configuration utility. This ability to start or stop services from within the Configuration utility is useful when you want to run only those services that you need to successfully manage network traffic.

The services that you might want to stop or start with the Configuration utility are:

- **ntpd**
  Sets and maintains the system time of day.
- **postfix**
  An alternative to the sendmail utility, sends and receives email.
- **radvd**
  Used by hosts to configure their interfaces, listens to router solicitations, and answers with router advertisement.
- **snmpd**
  Receives and processes SNMP requests, and sends trap notifications. Note that you must stop this service before updating the SNMP v3 file **/config/net-snmp/snmpd.conf**, which specifies SNMP user names.
- **sshd**
  Provides secure remote login between untrusted hosts.

For any services that you should run continually, such as the MCPD or TMM service, you cannot start or stop them using the Configuration utility. For more information on managing these essential services, see *Managing core services*, on page 18-2.

The Configuration utility screen for managing optional services lists the name of each service and its current status.

To stop, start, or restart an optional service

1. On the Main tab of the navigation pane, expand **System**, and click **Services**.
   The Services screen opens.
2. In the Service column, locate the name of the service you want to start, stop, or restart.
3. To the left of the service name, click the Select box.
4. Click **Start**, **Stop**, or **Restart**.
5. In the History column, check the status of the service.

◆ **Tip**

*You can also start and stop optional services using the **bigstart** utility. For more information, see the **bigstart** man page.*

A

Troubleshooting SNMP Traps

- Understanding F5-specific traps

Understanding F5-specific traps

The alert system and the SNMP agent on the BIG-IP system can send a number of notifications about the current operation of the BIG-IP system. The definitions of these notifications are known as ***traps***, and are contained in the MIB file **F5-BIGIP-COMMON-MIB.txt**.

The types of notifications that the BIG-IP system can send to an SNMP manager are:

- General traps
- Hardware-related traps
- License-related traps
- Traffic management operating system (TMOS)-related traps
- Authentication-related traps
- Denial of Service (DoS)-related traps
- Network-related traps
- Logging-related traps
- Application Security Module (ASM)-related traps
- Global Traffic Manager (GTM)-related traps
- Other traps

The remainder of this appendix contains tables that list the trap names contained in the MIB file **F5-BIGIP-COMMON-MIB.txt**, their descriptions, and the recommended action to take if you receive one of these notifications on your SNMP manager system.

General traps

The general notifications that you might receive on an SNMP manager system are listed and described in Table A.1.

Trap Name	Description	Recommended Action
bigipAgentStart	The SNMP agent on the BIG-IP system has been started.	For your information only. No action required.
bigipAgentShutdown	The SNMP agent on the BIG-IP system is in the process of being shut down.	
bigipAgent Restart	The SNMP agent on the BIG-IP system has been restarted.	This trap is for future use only and does not apply to BIG-IP system version 9.
bigipConfigLoaded	The BIG-IP system configuration data was successfully loaded.	For your information only. No action required.

Table A.1 *General traps and recommended actions*

Trap Name	Description	Recommended Action
bigipDiskPartitionWarn	Free space on the disk partition is limited, that is, less than a specified limit. By default, the limit is set to 30% of total disk space.	Increase the available disk space.
bigipDiskPartitionGrowth	The disk partition use exceeds the specified growth limit. By default, the limit is set to 5% of the total disk space.	

Table A.1 General traps and recommended actions

Hardware-related traps

The hardware-related notifications that you might receive on an SNMP manager system are listed and described in Table A.2.

Trap Name	Description	Recommended Action
bigipCpuTempHigh	The CPU temperature is too high.	Check the CPU and air temperatures. For BIG-IP platforms C36, D39, D44, D45, D50, D51, D51C, and D62, the threshold is 75 degrees Celsius. For the BIG-IP platform C62, the threshold is 80 degrees Celsius. If the condition persists, contact F5 Networks technical support.
bigipCpuFanSpeedLow	The CPU fan speed is too low.	Check the CPU temperature. If the CPU temperature is normal, the condition is not critical. For BIG-IP platforms C36, C62, D39, D44, D45, D50, D51, D51C, and D62, the threshold is 3000 RPM.
bigipCpuFanSpeedBad	The CPU fan is not receiving a signal.	Check the CPU temperature and verify that the CPU fan is plugged in and receiving power. If the CPU temperature is normal, the condition is not critical.
bigipChassisTempHigh	The temperature of the chassis is too high.	Check the chassis and air temperatures. For BIG-IP platforms C36, D39, D44, D45, D50, D51, D51C, D62, and C62 switchboard, the threshold is 75 degrees Celsius. For the BIG-IP platform C62 non-switchboard, the threshold is 95 degrees Celsius for one chassis and 80 degrees Celsius for the other chassis. If the condition persists, contact F5 Networks technical support.
bigipChassisFanBad	The chassis fan is not operating properly.	Check the chassis temperature. Also check that the fan is receiving power, or replace the fan.

Table A.2 Hardware-related traps and recommended actions

Trap Name	Description	Recommended Action
bigipChassisPowerSupplyBad	The chassis power supply is not functioning properly.	Verify that the power supply is plugged in, or contact F5 Networks technical support. For a dual-power-supply system, one power supply might not be plugged in.
bigipHardDiskFailure	The hard disk is failing.	Power off the system and replace the hard disk. Contact F5 Networks technical support.

Table A.2 *Hardware-related traps and recommended actions*

License-related traps

The notifications related to licensing that you might receive on an SNMP manager system are listed and described in Table A.3

Trap Name	Description	Recommended Action
bigipLicenseFailed	Validation of a BIG-IP system license has failed, or the dossier has errors. Occurs only when first licensing the system or adding a module key (such as HTTP compression) to an existing system.	If using automatic licensing, verify connectivity to the outside world, fix the dossier if needed, and try again.
bigipLicenseExpired	The BIG-IP license has expired.	Call F5 Networks technical support.

Table A.3 *License traps and recommended actions*

TMOS-related traps

The TMOS-related notifications that you might receive on an SNMP manager system are listed and described in Table A.4.

Trap Name	Description	Recommended Action
bigipServiceDown	A BIG-IP system health monitor has detected a service on a node to be stopped and has therefore marked the node as **down**.	Restart the service on the node.
bigipServiceUp	A BIG-IP system health monitor has detected a service on a node to be running and has therefore marked the node as **up**.	For your information only. No action required/
bigipNodeDown	A BIG-IP system health monitor has marked a node as **down**.	Check the node and the cable connection.

Table A.4 *TMOS-related traps and recommended actions*

Trap Name	Description	Recommended Action
bigipNodeUp	A BIG-IP system health monitor has marked a node as **up**.	For your information only. No action required.
bigipStandby	The BIG-IP system has switched to **standby** mode.	Review the log files in the **/var/log** directory and then search for core files in the **/var/core** directory. If you find a core file, or find text similar to **fault at location xxxx stack trace:**, contact F5 Networks technical support.
bigipStandByFail	In failover condition, this standby system cannot become active.	Investigate failover condition on the standby system.
bigipActive	The BIG-IP system has switched to **active** mode.	For your information only. No action required.
bigipActiveActive	The BIG-IP system is in **active-active** mode.	
bigipFeatureFailed	A high-availability feature has failed.	View high-availability processes and their current status using the BIG-IP system command **bigpipe ha table**.
bigipFeatureOnline	A high-availability feature is responding.	For your information only. No action required.
bigipPacketRejected	The BIG-IP system has rejected some packets.	Check the detailed message within this trap and act accordingly.

Table A.4 *TMOS-related traps and recommended actions*

Authentication-related traps

The notifications related to authentication that you might receive on an SNMP manager system are listed and described in Table A.5.

Trap Name	Description	Recommended Action
bigipTamdAlert	More than 60 authentication attempts have failed within one second, for a given virtual server.	Investigate for a possible intruder.
bigipAuthFailed	A login attempt failed.	Check the user name and password.

Table A.5 *Authentication traps and recommended actions*

DoS-related traps

The notifications related to denial of service that you might receive on an SNMP manager system are listed and described in Table A.6.

Trap Name	Description	Recommended Action
bigipAggrReaperStateChange	The state of the aggressive reaper has changed, indicating that the BIG-IP system is moving to a distress mode.	We recommend that you use our default Denial of Service settings. However, you can add rate filters to survive the attack.

Table A.6 *Denial of Service traps and recommended actions*

Network-related traps

The network-related notifications that you might receive on an SNMP manager system are listed and described in Table A.7.

Trap Name	Description	Recommended Action
bigipARPConflict	The BIG-IP system has detected an ARP advertisement for any of its own ARP-enabled addresses. This can occur for a virtual server address or a self IP address.	Check IP addresses and routes.
bigipNetLinkDown	An interface link is down. This applies to L1 and L2, which are internal links within the box connecting the CPU and Switch subsystems. These links should never be down. If this occurs, the condition is serious.	Contact F5 Networks technical support.

Table A.7 *Network traps and recommended actions*

Logging-related traps

The notifications related to logging that you might receive on an SNMP manager system are listed and described in Table A.8.

Trap Name	Description	Recommended Action
bigipLogEmerg	The BIG-IP system is unusable. This notification occurs when the system logs a message with the log level **LOG_EMERG**.	Check the detailed message within this trap and within the **/var/log** files to determine which process has the emergency. Then act accordingly.
bigipLogAlert	You must take action immediately for the BIG-IP system to function properly. This notification occurs when the system logs a message with the log level **LOG_ALERT**.	Check the detailed message within this trap and within the **/var/log** files to determine which process has the alert situation. Then act accordingly.
bigipLogCrit	The BIG-IP system is in a critical condition. This notification occurs when the system logs a message with the log level **LOG_CRIT**.	Check the detailed message within this trap and within the **/var/log** files to determine which process has the critical situation. Then act accordingly.
bigipLogErr	The BIG-IP system has some error conditions. This notification occurs when the system logs a message with the log level **LOG_ERR**.	Check the detailed message within this trap and within the **/var/log** files to determine which processes have the error conditions. Then act accordingly.
bigipLogWarning	The BIG-IP system is experiencing some warning conditions. This notification occurs when the system logs a message with the log level **LOG_WARNING**.	Check the detailed message within this trap and within the **/var/log** files to determine which processes have the warning conditions. Then act accordingly.

Table A.8 *Logging-related traps and recommended actions*

◆ **Note**

You can also view logging information using the Logs screen of the Configuration utility.

ASM-related traps

The notifications related to Application Security Module (ASM) that you might receive on an SNMP manager system are listed and described in Table A.6.

Trap Name	Description	Recommended Action
bigipAsmRequestBlocked	The system blocked an HTTP request because the request contained at least one violation to the active security policy.	Check the HTTP request to determine the cause of the violation.
bigipAsmRequestViolation	The system issued an alert because an HTTP request violated the active security policy.	Check the HTTP request to determine the cause of the violation.

Table A.9 *ASM traps and recommended actions*

GTM-related traps

The notifications related to Global Traffic Manager (GTM) that you might receive on an SNMP manager system are listed and described in Table A.6.

Trap Name	Description	Recommended Action
bigipGtmPoolAvail	A pool is becoming available in the GTM module.	For your information only. No action required.
bigipGtmPoolNotAvail	A pool is becoming unavailable in the GTM module.	Check the status of the pool, as well as the relevant detailed log message.
bigipGtmPoolDisabled	A pool is disabled in the GTM module.	Check the status of the pool.
bigipGtmPoolEnabled	A pool is enabled in the GTM module.	For your information only. No action required.
bigipGtmLinkAvail	A link is becoming available in the GTM module.	
bigipGtmLinkNotAvail	A link is becoming unavailable in the GTM module.	Check the status of the link, as well as the relevant detailed log message.
bigipGtmLinkDisabled	A link is disabled in the GTM module.	Check the status of the link.
bigipGtmLinkEnabled	A link is enabled in the GTM module.	For your information only. No action required.
bigipGtmWideIpAvail	A wide IP is becoming available in the GTM module.	

Table A.10 *GTM traps and recommended actions*

Trap Name	Description	Recommended Action
bigipGtmWideIpNotAvail	A wide IP is becoming unavailable in the GTM module.	Check the status of the wide IP, as well as the relevant detailed log message.
bigipGtmWideIpDisabled	A wide IP is disabled in the GTM module.	Check the status of the wide IP.
bigipGtmWideIpEnabled	A wide IP is enabled in the GTM module.	For your information only. No action required.
bigipGtmPoolMbrAvail	A pool member is becoming available in the GTM module.	
bigipGtmPoolMbrNotAvail	A pool member is becoming unavailable in the GTM module.	Check the status of the pool member, as well as the relevant detailed log message.
bigipGtmPoolMbrDisabled	A pool member is disabled in the GTM module.	Check the status of the pool member.
bigipGtmPoolMbrEnabled	A pool member is enabled in the GTM module.	For your information only. No action required.
bigipGtmServerAvail	A server is becoming available in the GTM module.	
bigipGtmServerNotAvail	A server is becoming unavailable in the GTM module.	Check the status of the server, as well as the relevant detailed log message.
bigipGtmServerDisabled	A server is disabled in the GTM module.	Check the status of the server.
bigipGtmServerEnabled	A server is enabled in the GTM module.	For your information only. No action required.
bigipGtmVsAvail	A virtual server is becoming available in the GTM module.	
bigipGtmVsNotAvail	A virtual server is becoming unavailable in the GTM module.	Check the status of the virtual server, as well as the relevant detailed log message.
bigipGtmVsDisabled	A virtual server is disabled in the GTM module.	Check the status of the virtual server.
bigipGtmVsEnabled	A virtual server is enabled in the GTM module.	For your information only. No action required.
bigipGtmDcAvail	A data center is becoming available in the GTM module.	
bigipGtmDcNotAvail	A data center is becoming unavailable in the GTM module.	Check the status of the data center, as well as the relevant detailed log message.
bigipGtmDcDisabled	A data center is disabled in the GTM module.	Check the status of the data center.

Table A.10 *GTM traps and recommended actions*

Trap Name	Description	Recommended Action
bigipGtmDcEnabled	A data center is enabled in the GTM module.	For your information only. No action required.
bigipGtmAppObjAvail	An application object is becoming available in the GTM module.	
bigipGtmAppObjNotAvail	An application object is becoming unavailable in the GTM module.	Check the status of the application object, as well as the relevant detailed log message.
bigipGtmAppAvail	An application is becoming available in the GTM module.	For your information only. No action required.
bigipGtmAppNotAvail	An application is becoming unavailable in the GTM module.	Check the status of the application, as well as the relevant detailed log message.
bigipGtmJoinedGroup	The GTM module joined a sync group.	For your information only. No action required.
bigipGtmLeftGroup	The GTM module left a sync group.	

Table A.10 *GTM traps and recommended actions*

Other traps

Other notifications that you might receive on an SNMP manager system are listed and described in Table A.6.

Trap Name	Description	Recommended Action
bigipCompLimitExceeded	The compression license limit is exceeded.	Purchase additional compression licensing from F5 Networks.
bigipSslLimitExceeded	The SSL license limit is exceeded, either for transactions per second (TPS) or for megabits per second (MPS).	Purchase additional SSL licensing from F5 Networks.
bigipExternalLinkChange	The status of an external interface link has changed to either **DOWN** or **UP**. This occurs when network cables are added or removed, and the network is reconfigured.	Determine whether the link should be down or up, and then take the appropriate action.

Table A.11 *Other traps and recommended actions*

B

Configuring bigdb Database Keys

- Introducing the bigdb database
- Summarizing bigdb keys for redundant system administration
- Summarizing bigdb keys for user account administration
- Summarizing bigdb keys for event logging

Introducing the bigdb database

Every BIG-IP system includes a bigdb^{TM} database. The bigdb database holds a set of ***bigdb configuration keys***, which define the behavior of various aspects of the BIG-IP system. For example, the bigdb key **Failover.Active Mode**, when set to **enable**, causes a redundant system to operate in active-active mode, instead of the default active/standby mode.

You can change the value of a bigdb key in two ways:

- **The Configuration utility**
  When you use the Configuration utility to configure various BIG-IP features, you are actually resetting bigdb key values. In this case, the bigdb keys are invisible to users.
- **The bigpipe db command**
  You can reset bigdb key values directly using the **bigpipe db** command. This command is useful if you prefer not to use the Configuration utility to configure a BIG-IP feature, or if configuration of a particular aspect of BIG-IP system behavior is not available through the Configuration utility. The syntax for displaying and setting bigdb keys is:

  ```
  bigpipe db all list
  bigpipe db <key name> <value>
  ```

Tip

*For more information on using the **bigpipe db** command, see the online man page for the command.*

Some of the bigdb database keys for system management that you might want to configure pertain specifically to redundant systems and user accounts.

Summarizing bigdb keys for redundant system administration

There are several bigdb keys that you can use to configure and manage a redundant system. These keys pertain to the following redundant-system features:

- Failover
- Connection mirroring
- Configuration synchronization
- System fail-safe

Using failover keys

The bigdb keys that you can configure for failover are shown in Table B.1, on page B-2. These keys are listed in alphabetical order.

Key Name	Default Value	Description
Failover.ActiveMode	**disable**	Enables or disables active-active mode. Use active-active mode if set to **1**. By default, this is **0** (off) and active/standby mode is used. Possible values are **enable** and **disable**.
Failover.DbgFile	**/var/log/sodlog**	Specifies the file into which the **sod** service logs the failover debug information.
Failover.FailbackDelay	**60**	For an active-active system, when the failed unit becomes active again, specifies the number of seconds that you want the system to wait before failback occurs.
Failover.FailedStandbyActive	**disable**	Controls whether a standby unit with a failover condition becomes active when the peer unit fails. Possible values are **enable** and **disable**.
Failover.ForceActive	**disable**	Specifies that the failover daemon should always attempt to become the active unit. Possible values are **enable** and **disable**.
Failover.ForceStandby	**disable**	Specifies that the failover daemon should switch to a standby state whenever the current unit senses that its peer is alive. Possible values are **enable** and **disable**.
Failover.IsRedundant	**false**	Defines whether the BIG-IP system is a unit of a redundant pair. Possible values are **true** and **false**.
Failover.ManFailBack	**disable**	If using active-active mode, specifies that the system should wait until the surviving unit receives a command before surrendering resources to a rebooted machine. Possible values are **enable** and **disable**.

Table B.1 *bigdb database keys pertaining to failover*

Key Name	Default Value	Description
Failover.MemoryRestartPercent	**97**	Defines the amount of memory usage that causes the BIG-IP system to reboot.
Failover.Network	**0**	Specifies whether the system should use the network as a backup to, or instead of, the hard-wired connection for failover. Possible values are **0** (off) and **1** (on).
Failover.PrintPeerState	**disable**	Specifies that the failover daemon (**/sbin/sod**) should write the state of its connection (hard-wired or network) to its peer. The system writes this information to the failover daemon's debug log file. Possible values are **enable** and **disable**.
Failover.Standby.LinkDownTime	**0**	Defines the amount of time in seconds that the system's interfaces are down before switching to a standby state.
Failover.UnitId	**1**	Specifies the ID of the unit. Each BIG-IP system must have a unique unit ID of **1** or **2** in the event that network communication is not possible with its peer.
Failover.UseTty00	**disable**	Specifies that the failover daemon should use **/dev/tty00** for hard-wired failover. Possible values are **enable** and **disable**.
Failover.UseTty01	**disable**	Specifies that the failover daemon should use **/dev/tty01** for hard-wired failover. Possible values are **enable** and **disable**.

Table B.1 *bigdb database keys pertaining to failover*

Using connection mirroring keys

The bigdb keys that you can configure for connection mirroring are shown in Table B.2. These keys are listed in alphabetical order.

Key Name	Default Value	Description
StateMirror.Ipaddr	No default value	Specifies the unit's primary static self IP address that its peer uses to mirror connections.
StateMirror.PeerIpaddr	No default value	Specifies the peer unit's primary static self IP address that a unit uses to mirror connections.
StateMirror.PeerListenPort	**1028**	Defines the port on which the BIG-IP system listens for connections from the active unit.
StateMirror.Secondary.Ipaddr	No default value	Specifies the unit's secondary static self IP address that its peer uses to mirror connections.

Table B.2 *bigdb database keys pertaining to connection mirroring*

Key Name	Default Value	Description
StateMirror.SecondaryPeerIpaddr	No default value	Specifies the peer unit's secondary static self IP address that a unit uses to mirror connections.
StateMirror.State	**enable**	Defines whether connection mirroring is enabled or disabled for a redundant system. Possible values are **enable** and **disable**.

Table B.2 *bigdb database keys pertaining to connection mirroring*

Using configuration synchronization keys

The bigdb keys that you can configure for synchronizing configuration data are shown in Table B.3. These keys are listed in alphabetical order.

Key Name	Default Value	Description
Configsync.Autodetect	**enable**	Defines whether the Configuration utility should automatically detect configuration status and display it on all Configuration utility screens. Possible values are **enable** and **disable**.
Configsync.LocalConfigTime	**0**	Specifies the most recent date and time that the configuration of the current unit changed.
Configsync.LocalSyncedTime	**0**	Specifies the date and time that the configuration of this unit was synchronized with the peer unit.
Configsync.password	No default value	Defines the password of the user account that has permission to synchronize configuration data.
Configsync.PeerConfigTime	**0**	Specifies the most recent date and time that the configuration of the peer unit changed.
Configsync.PeerState	**unknown**	Defines whether the peer's synchronization state is known. Possible values are **known** and **unknown**.
Configsync.PeerUpdatedTime	**0**	Specifies the date and time that this unit successfully informed its peer of a configuration change on this unit.

Table B.3 *bigdb database keys pertaining to configuration synchronization*

Key Name	Default Value	Description
Configsync.State	**-1**	Specifies the configuration state of this box. Possible values are: **-1** - Uninitiated or disabled config state. **0** - Synchronized. **1** - Configuration on current unit was modified. Recommend configuration synchronization to peer unit. **2** - Configuration on peer unit was modified. Recommend configuration synchronization from peer unit. **3** - Configuration modified on both units. Manual intervention required.
Configsync.username	**admin**	Defines the user account that has permission to synchronize configuration data.

Table B.3 *bigdb database keys pertaining to configuration synchronization*

Using system fail-safe keys

The bigdb keys that you can configure for system fail-safe are shown in Table B.4. These keys are listed in alphabetical order.

Key Name	Default Value	Description
Switchboard.Failsafe	**enable**	Enables or disables fail-safe when the switch board fails. Possible values are **enable** and **disable**.
Switchboard.Failsafe.Action	**failover**	Specifies the action that the system takes when the switch board fails. Possible values are **failover**, **reboot**, and **restart_all**.

Table B.4 *bigdb database keys pertaining to system fail-safe*

Summarizing bigdb keys for user account administration

You can configure a set of bigdb keys to manage administrative user accounts for a BIG-IP system. These keys and their descriptions appear in Table B.5, and are listed in alphabetical order.

Key Name	Default Value	Description
User.AcceptedEULA	**none**	Specifies fields that the Setup utility populates. Possible values are **none**, **internal**, **non-production**, and **production**.
Users.Default.Role	**127**	Specifies a numeric value for the default role for remote user accounts.
Users.LocalOnly	**root**,**admin**	Specifies those user accounts that must reside locally on the BIG-IP system and therefore cannot reside on a remote authentication server.
Users.Name.admin	**0**	Specifies a numeric value for the **admin** account.
Users.Name.support	**0**	Specifies a numeric value for the **support** account.
Users.Name.[user name]	**127**	Specifies a numeric value for any user account that is not **root**, **admin**, or **support**.

Table B.5 *bigdb database keys pertaining to user accounts*

Summarizing bigdb keys for event logging

The bigdb keys that you can configure to set the minimum log level on local traffic and authentication events are shown in Table B.6. These keys are listed in alphabetical order. For information on all possible key values, see Chapter 17, *Logging BIG-IP System Events*.

Key Name	Default Value	Description
Bigdb.loglevel	**Informational**	Sets the minimum log level for events related to populating and persisting bigdb database variables.
log.arp.level	**Warning**	Sets the minimum log level for events related to ARP packets and the ARP cache. These events include IPv6 neighbor discovery events.
log.config.level	**Notice**	Sets the minimum log level for MCP events related to configuring the Traffic Management Microkernel (TMM).
log.deflate.level	**Error**	Sets the minimum log level for events related to HTTP compression.
log.http.level	**Error**	Sets the minimum log level for events related to HTTP protocol processing.
log.ipnet.level	**Notice**	Sets the minimum log level for events related to packets discarded due to exceptional circumstances, such as bad checksums or unhandled protocol versions.
log.layer4.level	**Notice**	Sets the minimum log level for events related to TCP, UDP, and FastL4 protocol and packet processing.
log.net.level	**Warning**	Sets the minimum log level for events related to layer 1 and layer 2 processing.
log.pva.level	**Informational**	Sets the minimum log level for events generated by the Packet Velocity® ASIC service **pvad**.
log. rules.level	**Informational**	Sets the minimum log level for events related to run-time processing or iRules.
log.ssl.level	**Warning**	Sets the minimum log level for events related to SSL protocol processing.
log.tmm.level	**Notice**	Sets the minimum log level for general events such as TMM startup and shutdown.

Table B.6 *bigdb database keys pertaining to setting log levels*

Summarizing bigdb keys for HTTP compression

You can configure a set of bigdb keys to manage the way that the BIG-IP system handles the compression of HTTP server responses. These keys and their descriptions appear in Table B.7, and are listed in alphabetical order.

Key Name	Default Value	Description
Compression.Hardware.Ratio	**4**	Used only when the **Compression.Strategy** key is set to **ratio**. This ratio defines how each compressible response is load balanced between compression devices.
Compression.Offload.Ratio	**4**	Used only when the **Compression.Strategy** key is set to **ratio**. This ratio defines how each compressible response is load balanced between compression devices.
Compression.Strategy	**speed**	Sets the way that the system directs traffic flow. Possible values are **speed**, **size**, and **ratio**: **speed** - The system uses the hardware to the fullest extent possible. The **speed** value is best used for bulk compression and for limiting CPU overhead. **size** - When the key is set to the **size** value, the system performs as much compression in the software as possible. Normally, the system uses a ratio of TMM and Offload. When both are busy, compression is performed in the hardware. The **size** value gives the best ratio at the expense of CPU overhead. **ratio** - The system uses the three bigdb keys **Compression.Hardware.Ratio**, **Compression.Offload.Ratio**, and **Compression.TMM.Ratio**, with the goal of limiting CPU overhead while giving good compression ratios.
Compression.TMM.Ratio	**1**	Used only when the **Compression.Strategy** key is set to **ratio**. This ratio defines how each compressible response is load balanced between compression devices.

Table B.7 *bigdb database keys pertaining to HTTP data compression*

Glossary

active unit

In a redundant system, the active unit is the system that currently load balances connections. If the active unit in the redundant system fails, the standby unit assumes control and begins to load balance connections. See also *redundant system*.

archive

An archive is a backup copy of the BIG-IP system configuration data. This archive is in the form of a user configuration set, or UCS. See also *user configuration set (UCS)*.

ARP (Address Resolution Protocol)

ARP is an industry-standard protocol that determines a host's Media Access Control (MAC) address based on its IP address.

ARP cache

The ARP (address resolution protocol) cache is the mechanism that a device on a network uses to determine the MAC address of another device, when only the IP addrsess of that other device is known.

authentication

Authentication is the process of verifying a user's identity when the user is attempting to log on to a system.

authentication iRule

An authentication iRule is a system-supplied or user-created iRule that is necessary for implementing a PAM authentication module on the LTM system. See also *iRule*, *PAM (Pluggable Authentication Module)*.

authentication module

An authentication module is a PAM module that you create to perform authentication or authorization of client traffic. See also *PAM (Pluggable Authentication Module)*.

authentication profile

An authentication profile is a configuration tool that you use to implement a PAM authentication module. Types of authentication modules that you can implement with an authentication profile are: LDAP, RADIUS, TACACS+, SSL Client Certificate LDAP, and OCSP. See also *PAM (Pluggable Authentication Module)*.

authorization

Authorization is the process of identifying the level of access that a logged-on user has been granted to system resources.

bigtop

The **bigtop** utility is a statistical monitoring utility that ships on the BIG-IP system. This utility provides real-time statistical information.

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**.

BPDU (bridge protocol data unit)

A BPDU is a special packet that a spanning tree protocol sends between layer 2 devices to determine redundant paths, and provide loop resolution. See also *STP (Spanning Tree Protocol)*, *RSTP (Rapid Spanning Tree Protocol)*, and *MSTP (Multiple Spanning Tree Protocol).*

bridge

A bridge is a layer 2 networking device that defines a collision domain.

bursting

Bursting is an aspect of rate shaping and occurs when the rate of traffic flow exceeds the base rate defined.

certificate

A certificate is an online credential signed by a trusted certificate authority and used for SSL network traffic as a method of authentication.

certificate authority (CA)

A certificate authority is an external, trusted organization that issues a signed digital certificate to a requesting computer system for use as a credential to obtain authentication for SSL network traffic.

certificate revocation list (CRL)

A certificate revocation list is a list that an authenticating system checks to see if the SSL certificate that the requesting system presents for authentication has been revoked.

certificate verification

Certificate verification is the part of an SSL handshake that verifies that a client’s SSL credentials have been signed by a trusted certificate authority.

chain

A chain is a series of filtering criteria used to restrict access to an IP address. The order of the criteria in the chain determines how the filter is applied, from the general criteria first, to the more detailed criteria at the end of the chain.

chunking

See *HTTP chunking*.

cipher

A cipher is an encryption/decryption algorithm that computer systems use when transmitting data using the SSL protocol.

client-side SSL profile

A client-side SSL profile is an SSL profile that controls the behavior of SSL traffic going from a client system to the LTM system.

clone pool

This feature causes a pool to replicate all traffic coming into it and send that traffic to a duplicate pool.

configuration object

A configuration object is a user-created object that the LTM system uses to implement a PAM authentication module. There is one type of configuration object for each type of authentication module that you create. See also *PAM (Pluggable Authentication Module)*.

configuration synchronization

Configuration synchronization is the task of duplicating a BIG-IP system's configuration data onto its peer unit in a redundant system.

Configuration utility

The Configuration utility is the browser-based application that you use to configure the LTM system.

connection persistence

Connection persistence is an optimization technique whereby a network connection is intentionally kept open for the purpose of reducing handshaking.

connection pooling

Connection pooling is an optimization feature that pools server-side connections for re-use by other client requests. Connection pooling reduces the number of new connections that must be opened for server-side client requests.

content switching

Content switching is the ability to select a pool based on data contained within a packet.

cookie persistence

Cookie persistence is a mode of persistence where the LTM system stores persistent connection information in a cookie.

custom profile

A custom profile is a profile that you create. A custom profile can inherit its default settings from a parent profile that you specify. See also *parent profile*.

data group

A data group is a group of related elements, such as a set of IP addresses for AOL clients. When you specify a data group along with the **matchclass** command or the **contains** operator, you eliminate the need to list multiple values as arguments in an iRule expression.

default profile

A default profile is a profile that the LTM system supplies with default setting values. You can use a default profile as is, or you can modify it. You can also specify it as a parent profile when you create a custom profile. You cannot create or delete a default profile. See also *profile*, *custom profile*.

default route

A default route is the route that the system uses when no other route specified in the routing table matches the destination address or network of the packet to be routed.

ddefault VLAN

The LTM system is configured with two default VLANs, one for each interface. One default VLAN is named **internal** and one is named **external**. See also *VLAN (virtual local area network)*.

default wildcard virtual server

A default wildcard virtual server has an IP address and port number of **0.0.0.0:0**. or ***:*** or **"any":"any"**. This virtual server accepts all traffic that does not match any other virtual server defined in the configuration.

destination address affinity persistence

Also known as sticky persistence, destination address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the destination IP address of a packet.

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.siterequest.com/index.html**, the domain name is **siterequest.com**.

Dynamic Ratio load balancing method

Dynamic Ratio mode is like Ratio mode (see *Ratio method*), except that ratio weights are based on continuous monitoring of the servers and are therefore continually changing. Dynamic Ratio load balancing can be implemented on RealNetworks® RealServer platforms, on Microsoft® Windows® platforms equipped with Windows Management Instrumentation (WMI), or on a server equipped with either the UC Davis SNMP agent or Windows 2000 Server SNMP agent.

dynamic route

A dynamic route is a route that an advanced routing protocol such as RIP adds dynamically to a routing table. See also *static route*.

EAV (Extended Application Verification)

EAV is a health check that verifies an application on a node by running that application remotely. EAV health check is only one of the three types of health checks available on an LTM system. See also *health check*, *health monitor*, and *external monitor*.

ECV (Extended Content Verification)

ECV is a health check that allows you to determine if a node is **up** or **down** based on whether the node returns specific content. ECV health check is only one of the three types of health checks available on an LTM system. See also *health check*.

external authentication

External authentication refers to the process of using a remote server to store data for the purpose of authenticating users or applications attempting to access the LTM system.

external monitor

An external monitor is a user-supplied health monitor. See also *health check*, *health monitor*.

external VLAN

The external VLAN is a default VLAN on the BIG-IP system. In a basic configuration, this VLAN has the administration ports locked down. In a normal configuration, this is typically a VLAN on which external clients request connections to internal servers.

failback

Failback is the process whereby an active unit relinquishes processing to a previously-failed unit that is now available.

failover

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

failover cable

The failover cable directly connects the two units together in a redundant system.

Fastest method

Fastest mode is a load balancing method that passes a new connection based on the fastest response of all currently active nodes.

FDDI (Fiber Distributed Data Interface)

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

floating self IP address

A floating self IP address is an additional self IP address for a VLAN that serves as a shared address by both units of a BIG-IP redundant system.

forwarding virtual server

A forwarding virtual server is a virtual server that has no pool members to load balance. The virtual server simply forwards the packet directly to the destination IP address specified in the client request. See also *virtual server*.

gateway pool

A gateway pool is a pool of routers that you can create to forward traffic. After creating a gateway pool, you can specify the pool as a gateway, within a TMM routing table entry.

hash persistence

Hash persistence allows you to create a persistence hash based on an existing iRule.

health check

A health check is an LTM system feature that determines whether a node is **up** or **down**. Health checks are implemented through health monitors. See also *health monito*r, *ECV*, *EAV*, and *external monitor*.

health monitor

A health monitor checks a node to see if it is **up** and functioning for a given service. If the node fails the check, it is marked **down**. Different monitors exist for checking different services. See also *health check*, *EAV, ECV,* and *external monitor*.

host virtual server

A host virtual server is a virtual server that represents a specific site, such as an Internet web site or an FTP site, and it load balances traffic targeted to content servers that are members of a pool.

HTTP chunking

HTTP chunking refers to the HTTP/ 1.1 feature known as chunked encoding, which allows HTTP messages to be broken up into several parts. Chunking is most often used by servers when sending responses.

HTTP redirect

An HTTP redirect sends an **HTTP 302 Object Found** message to clients. You can configure a pool with an HTTP redirect to send clients to another node or virtual server if the members of the pool are marked **down**.

HTTP transformation

When the LTM system performs an HTTP transformation, the system manipulates the **Connection** header of a server-side HTTP request, to ensure that the connection stays open. See also *connection persistence*.

ICMP (Internet Control Message Protocol)

ICMP is an Internet communications protocol used to determine information about routes to destination addresses.

i-mode

i-mode® is a service created by NTT DoCoMo, Inc., that allows mobile phone users access to the Internet.

interface

A physical port on a BIG-IP system is called an interface.

internal VLAN

The internal VLAN is a default VLAN on the BIG-IP system. In a basic configuration, this VLAN has the administration ports open. In a normal configuration, this is a network interface that handles connections from internal servers.

IPSEC

IPSEC (Internet Security Protocol) is a communications protocol that provides security for the network layer of the Internet without imposing requirements on applications running above it.

iRule

An iRule™ is a user-written script that controls the behavior of a connection passing through the LTM system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence.

iSNAT (intelligent SNAT)

An iSNAT is the mapping of one or more original client IP addresses to a translation address from within an iRule. Before writing an iRule to create an iSNAT, you must create a SNAT pool. See also *SNAT pool*.

JAR file

A JAR file is a file in Java™ Archive (JAR) file format that enables you to bundle multiple files into a single archive file. Typically, a JAR file contains the class files and auxiliary resources associated with applets and applications.

JDBC

JDBC is a Java™ technology. It is an application programming interface that provides database management system (DBMS) connectivity across a wide range of SQL databases, as well as access to other tabular data sources, such as spreadsheets or flat files.

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.

LACP (Link Aggregation Control Protocol)

LACP is an industry-standard protocol that aggregates links in a trunk, to increase bandwidth and provide for link failover.

last hop

A last hop is the final hop a connection takes to get to the BIG-IP system. You can allow the BIG-IP system to determine the last hop automatically to send packets back to the device from which they originated. You can also specify the last hop manually by making it a member of a last hop pool.

layer 1 through layer 7

Layers 1 through 7 refer to the seven layers of the Open System Interconnection (OSI) model. Thus, layer 2 represents the data-link layer, layer 3 represents the IP layer, and layer 4 represents the transport layer (TCP and UDP). Layer 7 represents the application layer, handling traffic such as HTTP and SSL.

layer 2 forwarding table

A layer 2 forwarding table correlates MAC addresses of network devices to the BIG-IP system interfaces through which those devices are accessible. On a BIG-IP system, each VLAN has its own layer 2 forwarding table.

LDAP (Lightweight Directory Access Protocol)

LDAP is an Internet protocol that email programs use to look up contact information from a server.

LDAP authentication module

An LDAP authentication module is a user-created module that you implement on an LTM system to authenticate client traffic using a remote LDAP server.

LDAP client certificate SSL authentication module

An LDAP client certificate SSL authentication module is a user-created module that you implement on an LTM system to authorize client traffic using SSL client credentials and a remote LDAP server.

Least Connections method

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

link aggregation

Link aggregation is the process of combining multiple links in order to function as though it were a single link with higher bandwidth. Link aggregation occurs when you create a trunk. See also *trunk* and *LACP (Link Aggregation Control Protocol)*.

load balancing method

A particular method of determining how to distribute connections across a load balancing pool.

load balancing pool

See *pool*.

load balancing virtual server

A load balancing virtual server is a virtual server that directs client traffic to a load balancing pool. This is the most basic type of virtual server. See also *virtual server*.

local traffic management (LTM)

Local traffic management (LTM) is the process of managing network traffic that comes into or goes out of a local area network (LAN), including an intranet.

loopback adapter

A loopback adapter is a software interface that is not associated with an actual network card. The nPath routing configuration requires you to configure loopback adapters on servers.

MAC (Media Access Control)

MAC is a protocol that defines the way workstations gain access to transmission media, and is most widely used in reference to LANs. For IEEE LANs, the MAC layer is the lower sublayer of the data link layer protocol.

MAC address

A MAC address is used to represent hardware devices on an Ethernet network.

management interface

The management interface is a special port on the BIG-IP system, used for managing administrative traffic. Named **MGMT**, the management interface does not forward user application traffic, such as traffic slated for load balancing. See also *TMM switch interface*.

management route

A management route is a route that forwards traffic through the special management (**MGMT**) interface.

MCPD service

The Master Control Program Daemon (MCPD) service manages the configuration data on a BIG-IP system.

MindTerm SSH

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

minimum active members

The minimum active members is the number of members that must be active in a priority group in order for the LTM system to send its requests to that group. If the number of active members falls below this number, requests are sent to the next highest priority group (the priority group with the next lowest priority number).

monitor

The LTM system uses monitors to determine whether nodes are **up** or **down**. There are several different types of monitors and they use various methods to determine the status of a server or service.

monitor association

A monitor association is an association that a user makes between a health or performance monitor and a pool, pool member, or node.

monitor instance

You create a monitor instance when a health monitor is associated with a pool member or node. It is the monitor instance that actually performs the health check, not the monitor.

monitor template

A monitor template is an internal mechanism that the LTM system uses to provide default values for a custom monitor when no pre-configured monitor exists.

MSRDP persistence

MSRDP persistence tracks sessions between clients and servers running the Microsoft® Remote Desktop Protocol (RDP) service.

MSTP (Multiple Spanning Tree Protocol)

Defined by IEEE, MSTP is an enhanced spanning tree protocol. Unlike STP and RSTP, MSTP is VLAN-aware and therefore incorporates the concept of MSTP regions. See also *STP (Spanning Tree Protocol*) and *RSTP (Rapid Spanning Tree Protocol).*

MSTP region

An ***MSTP region*** is a group of layer 2 devices that have identical values for certain configuration settings. When devices constitute a region, the spanning tree algorithm takes VLANs into account when blocking and unblocking redundant paths.

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.

NAT (Network Address Translation)

A NAT is an alias IP address that identifies a specific node managed by the LTM system to the external network.

network virtual server

A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is **0**). There are two kinds of network virtual servers: those that direct client traffic based on a range of destination IP addresses, and those that direct client traffic based on specific destination IP addresses that the LTM system does not recognize.

node

A node address is the IP address associated with one or more nodes. This IP address can be the real IP address of a network server, or it can be an alias IP address on a network server.

node alias

A node alias is a node address that the LTM system uses to verify the status of multiple nodes. When the LTM system uses a node alias to check node status, it pings the node alias. If the LTM system receives a response to the ping, it marks all nodes associated with the node alias as **up**. If the LTM system does not receive a response to the ping, it marks all nodes associated with the node alias as **down**.

node port

A node port is the port number or service name that is hosted by a specific node.

node status

Node status indicates whether a node is **up** and available to receive connections, or **down** and unavailable. The LTM system uses the node ping and health check features to determine node status.

Observed method

Observed mode is a dynamic load balancing method that bases connection distribution on a combination of two factors: the server that currently hosts the fewest connections and also has the fastest response time.

OCSP (Online Certificate Status Protocol)

OCSP is a protocol that authenticating systems can use to check on the revocation status of digitally-signed SSL certificates. The use of OCSP is an alternative to the use of a certificate revocation list (CRL). See also *certificate revocation list (CRL).*

OCSP authentication module

An OCSP authentication module is a user-created module that you implement on an LTM system to authenticate client traffic using a remote OCSP responder. The purpose of an OCSP authentication module is to check on the revocation status of a client SSL certificate.

OCSP responder

An OCSP responder is an external server used for communicating SSL certificate revocation status to an authentication server such as the LTM system.

OCSP responder object

A responder object is a software application on the LTM system that communicates with an OCSP responder, for the purpose of checking revocation status of a client or server SSL certificate.

OneConnect™

The F5 Networks OneConnect™ feature optimizes the use of network connections by keeping server-side connections open and pooling them for re-use.

packet rate

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

PAM (Pluggable Authentication Module)

PAM is a software module that a server application uses to authenticate client traffic. The modular design of PAM allows an organization to add, replace, or remove that authentication mechanism from a server application with minimal impact to that application. An example of PAM is an application that uses a remote Lightweight Directory Access Protocol (LDAP) server to authenticate client traffic. See also *LDAP (Lightweight Directory Access Protocol)*.

parent profile

A parent profile is a profile that can propagate its values to another profile. A parent profile can be either a default profile or a custom profile. See also *profile*.

performance monitor

A performance monitor gathers statistics and checks the state of a target device.

persistence

See *connection persistence* or *session persistence*.

persistence profile

A persistence profile is a configuration tool for implementing a specific type of session persistence. An example of a persistence profile type is a cookie persistence profile.

pipelining

Pipelining is a feature of HTTP/1.1 that allows clients to make requests even when prior requests have not yet received a response from the server.

pool

A pool is composed of a group of network devices (called members). The LTM system load balances requests to the nodes within a pool based on the load balancing method and persistence method you choose when you create the pool or edit its properties.

pool member

A pool member is a server that is a member of a load balancing pool.

port

A port can be represented by a number that is associated with a specific service supported by a host. Refer to the Services and Port Index for a list of port numbers and corresponding services.

port mirroring

Port mirroring is a feature that allows you to copy traffic from any port or set of ports to a single, separate port where a sniffing device is attached.

port-specific wildcard virtual server

A port-specific wildcard virtual server is a wildcard virtual server that uses a port number other than **0**. See *wildcard virtual server*.

pre-configured monitor

A pre-configured monitor is a system-supplied health or performance monitor. You can use a pre-configured monitor as is, but you cannot modify or delete one. See also *monitor*.

Predictive method

Predictive mode is a dynamic load balancing method that bases connection distribution on a combination of two factors: the server that currently hosts the fewest connections, and also has the fastest response time. Predictive method also ranks server performance over time, and passes connections to servers which exhibit an improvement in performance rather than a decline.

profile

A profile is a configuration tool containing settings for defining the behavior of network traffic. The LTM system contains profiles for managing FastL4, HTTP, TCP, FTP, SSL, and RTSP traffic, as well as for implementing persistence and application authentication.

profile setting

A profile setting is a configuration attribute within a profile that has a value associated with it. You can configure a profile setting to customize the way that the LTM system manages a type of traffic.

profile type

A profile type is a category of profile that you use for a specific purpose. An example of a profile type is an HTTP profile, which you configure to manage HTTP network traffic.

protocol profile

A protocol profile is a profile that you create for controlling the behavior of FastL4, TCP, UDP, OneConnect, and RTSP traffic.

Quality of Service (QoS) level

The Quality of Service (QoS) level is a means by which network equipment can identify and treat traffic differently based on an identifier. Essentially, the QoS level specified in a packet enforces a throughput policy for that packet.

RADIUS (Remote Authentication Dial-in User Service)

RADIUS is a service that performs remote user authentication and accounting. Its primary use is for Internet Service Providers, though it can also be used on any network that needs a centralized authentication and/or accounting service for its workstations.

RADIUS authentication module

A RADIUS authentication module is a user-created module that you implement on an LTM system to authenticate client traffic using a remote RADIUS server.

RAM cache

A RAM cache is a cache of HTTP objects stored in the BIG-IP system's RAM that subsequent connections reuse to reduce the amount of load on the back-end servers.

rate class

You create a rate filter from the Configuration utility or command line utility. When you assign a rate class to a rate filter, a rate class determines the volume of traffic allowed through a rate filter. See also *rate shaping*.

rate shaping

Rate shaping is a type of extended IP filter. Rate shaping uses the same IP filter method but applies a rate class, which determines the volume of network traffic allowed. See also *rate class*.

ratio

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

Ratio method

The Ratio load balancing method distributes connections across an array of virtual servers in proportion to the ratio weights assigned to each individual virtual server.

Real-Time Stream Protocol (RTSP)

See *RTSP*.

receive expression

A receive expression is the text string that the LTM system looks for in the web page returned by a web server during an extended content verification (ECV) health check.

redundant system

Redundant system refers to a pair of units that are configured for fail-over. In a redundant system, there are two units, one running as the active unit and one running as the standby unit. If the active unit fails, the standby unit takes over and manages connection requests.

referenence link

A reference link is the lowest-numbered interface in a trunk and is used for link aggregation.

remote administrative IP address

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

responder object

See *OCSP responder object*.

RFC 1918 addresses

An RFC 1918 address is an address that is within the range of non-routable addresses described in the IETF RFC 1918.

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.

router

A router is a layer 3 networking device. If no VLANs are defined on the network, a router defines a broadcast domain.

RSTP (Rapid Spanning Tree Protocol)

Defined by IEEE, RSTP is an enhanced version of STP (Spanning Tree Protocol). RSTP provides faster spanning tree performance compared to STP. See also *STP* (*Spanning Tree Protocol)* and *MSTP (Multiple Spanning Tree Protocol)*.

RTSP

RTSP (Real-Time Streaming Protocol) establishes and controls one or more time-synchronized streams of continuous media such as audio or video.

secure network address translation (SNAT)

See *SNAT*. See also *iSNAT*.

self IP address

Self IP addresses are the IP addresses owned by the BIG-IP system that you use to access devices in VLANs. You assign self IP addresses to VLANs.

send string

A send string is the request that the LTM system sends to the web server during an extended content verification (ECV) health check.

server-side SSL profile

A server-side SSL profile is an SSL profile that controls SSL traffic going between an LTM system and a destination server system.

service

Service refers to services such as TCP, UDP, HTTP, and FTP.

services profile

A services profile is a configuration tool on the LTM system for managing either HTTP or FTP network traffic.

session persistence

A series of related connections received from the same client, having the same session ID. When persistence is enabled, an LTM system sends all connections having the same session ID to the same node, instead of load balancing the connections. Session persistence is not to be confused with *connection persistence*.

Setup utility

The Setup utility walks you through the initial system configuration process. You can run the Setup utility from the Configuration utility start page.

simple persistence

See *source address affinity persistence*.

SIP persistence

SIP persistence is a type of persistence used for servers that receive Session Initiation Protocol (SIP) messages sent through UDP. SIP is a protocol that enables real-time messaging, voice, data, and video.

SNAT (Secure Network Address Translation)

A SNAT is a feature you can configure on the LTM system. A SNAT defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network. See also *standard SNAT* and *iSNAT (intelligent SNAT)*.

SNAT pool

A SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self-IP addresses.

SNMP (Simple Network Management Protocol)

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

source address affinity persistence

Also known as simple persistence, source address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the source IP address of a packet.

source processing

Source processing means that the interface rewrites the source of an incoming packet.

spanning tree

A spanning tree is a logical tree structure of layer 2 devices on a network, created by a spanning tree protocol algorithm and used for resolving network loops.

spanning tree instance

A spanning tree instance is a specific, named spanning tree that a spanning tree protocol creates. See also *spanning tree protocols*.

spanning tree protocols

Spanning tree protocols are the IEEE-specified set of protocols known as Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). The BIG-IP system includes support for all of these protocols. See also *STP (Spanning Tree Protocol)*, *RSTP (Rapid Spanning Tree Protocol)*, and *MSTP (Multiple Spanning Tree Protocol)*.

SSH

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

SSL (Secure Sockets Layer)

SSL is a network communications protocol that uses public-key technology as a way to transmit data in a secure manner.

SSL persistence

SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID.

SSL profile

An SSL profile is a configuration tool that you use to terminate and initiate SSL connections from clients and servers.

standard SNAT

A standard SNAT is a SNAT that you implement by using the SNAT screens of the Configuration utility. See also *SNAT (Secure Network Address Translation)* and *iSNAT (intelligent SNAT)*.

standby unit

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

state mirroring

State mirroring is a feature on the LTM system that preserves connection and persistence information in a redundant system.

static route

A static route is a route that you must explicitly configure on a layer 3 device in its routing table. See also *dynamic route*.

static self IP address

A static self IP address is a self IP address that is not shared between two units of a redundant system.

sticky persistence

See *destination address affinity persistence*.

STP (Spanning Tree Protocol)

Defined by IEEE, STP is a protocol that provides loop resolution in configurations where one or more external switches are connected in parallel with the BIG-IP system. See also *RSTP* (*Rapid Spanning Tree Protocol)* and *MSTP* (*Multiple Spanning Tree Protocol)*.

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.

TACACS (Terminal Access Controller Access Control System)

TACACS is an older authentication protocol common to UNIX systems. TACACS allows a remote access server to forward a user's login password to an authentication server.

TACACS+

TACACS+ is an authentication mechanism designed as a replacement for the older TACACS protocol. There is little similarity between the two protocols, however, and they are therefore not compatible.

TACACS+ authentication module

A TACACS+ authentication module is a user-created module that you implement on an LTM system to authenticate client traffic using a remote TACACS+ server.

tagged interface

A tagged interface is an interface that you assign to a VLAN in a way that causes the system to add a VLAN tag into the header of any frame passing through that interface. Tagged interfaces are used when you want to assign a single interface to multiple VLANs. See also *VLAN (virtual local area network)*.

Tcl

Tcl (Tools Command Lanuage) is an industry-standard scripting language. On the LTM system, users use Tcl to write iRules^{TM}.

TMM (Traffic Management Microkernel) service

The TMM service is the process running on the BIG-IP system that performs most traffic management for the product.

TMM switch interface

A TMM switch interface is an interface that the BIG-IP system uses to forward user application traffic such as HTTP or SSL traffic. Thus, when load balancing application traffic, the BIG-IP system uses TMM switch interfaces. See also *management interface*.

TMM switch route

A Traffic Management Microkernel (TMM) switch route is a route that forwards traffic through the TMM switch interfaces and not the management interface.

transparent node

A transparent node appears as a router to other network devices, including the BIG-IP system.

trunk

A trunk is a logcial group of BIG-IP system interfaces. When you create a trunk, the BIG-IP system can aggregrate the corresponding links as a way to increase bandwidth.

trusted CA file

A trusted CA file is a file containing a list of certificate authorities that an authenticating system can trust when processing client requests for authentication. A trusted CA file resides on the authenticating system and is used for authenticating SSL network traffic.

Type of Service (ToS) level

The Type of Service (ToS) level is another means, in addition to the Quality of Service (QoS) level, by which network equipment can identify and treat traffic differently based on an identifier.

Universal Inspection Engine (UIE)

The Universal Inspection Engine (UIE) is a feature that offers universal persistence and universal content switching, to enhance your load balancing capabilities. The UIE contains a set of rule variables and functions for building expressions that you can specify in pool definitions and rules.

universal persistence

Universal persistence gives you the ability to persist on any string found within a packet. Also, you can directly select the pool member to which you want to persist.

user configuration set (UCS)

A user configuration set is a backup file that you create for the BIG-IP system configuration data. When you create a UCS, the BIG-IP system assigns a **.ucs** extension to the filename. See also *archives.*

user role

A user role is a type and level of access that you assign to a BIG-IP system user account. By assigning user roles, you can control the extent to which BIG-IP system administrators can view or modify the BIG-IP system configuration.

virtual address

A virtual address is an IP address associated with one or more virtual servers managed by the LTM system.

virtual port

A virtual port is the port number or service name associated with one or more virtual servers managed by the LTM system. A virtual port number should be the same TCP or UDP port number to which client programs expect to connect.

virtual server

Virtual servers are a specific combination of virtual address and virtual port, associated with a content site that is managed by an LTM system or other type of host server.

VLAN (virtual local area network)

A VLAN is a logical grouping of interfaces connected to network devices. You can use a VLAN to logically group devices that are on different network segments. Devices within a VLAN use layer 2 networking to communicate and define a broadcast domain.

VLAN group

A VLAN group is a logical container that includes two or more distinct VLANs. VLAN groups are intended for load balancing traffic in a layer 2 network, when you want to minimize the reconfiguration of hosts on that network. See also *VLAN (virtual local area network).*

VLAN name

A VLAN name is the symbolic name used to identify a VLAN. For example, you might configure a VLAN named **marketing**, or a VLAN named **development**. See also *VLAN (virtual local area network).*

VLAN tag

An IEEE standard, a VLAN tag is an identification number inserted into the header of a frame that indicates the VLAN to which the destination device belongs. VLAN tags are used when a single interface forwards traffic for multiple VLANs.

WAP (Wireless Application Protocol)

WAP is an application environment and set of communication protocols for wireless devices designed to enable manufacturer-, vendor-, and technology-independent access to the Internet and advanced telephony services.

watchdog timer card

A watchdog timer card is a hardware device that monitors the BIG-IP system for hardware failure.

wildcard virtual server

A wildcard virtual server is a virtual server that uses an IP address of **0.0.0.0**, ***** or **"any"**. A wildcard virtual server accepts connection requests for destinations outside of the local network. Wildcard virtual servers are included only in Transparent Node Mode configurations.

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**).

Index