

F5 Networks Training

Getting Started with BIG-IP Local Traffic Manager (LTM)

Part One: High Availability and Traffic
Processing

Lab Guide



Getting Started with BIG-IP Local Traffic Manager Lab Guide

Part One: High Availability and Traffic Processing

Lab Guide

Sixth Printing; August, 2017

This manual was written for BIG-IP® products version 13.0.

© 2017, F5 Networks, Inc. All rights reserved.



Support and Contact Information

Obtaining Technical Support

Web	support.f5.com (Ask F5)
Phone	(206) 272-6888
Email (support issues)	support@f5.com
Email (suggestions)	feedback@f5.com

Contacting F5 Networks

Web	www.f5.com
Email	sales@f5.com & info@f5.com

F5 Networks, Inc.

Corporate Office

401 Elliott Avenue West
Seattle, Washington 98119
T (888) 88BIG-IP
T (206) 272-5555
F (206) 272-5557
Training@f5.com

F5 Networks, Ltd.

United Kingdom

Chertsey Gate West
Chertsey Surrey KT16 8AP
United Kingdom
T (44) 0 1932 582-000
F (44) 0 1932 582-001
EMEATraining@f5.com

F5 Networks, Inc.

Asia Pacific

5 Temasek Boulevard
#08-01/02 Suntec Tower 5
Singapore, 038985
T (65) 6533-6103
F (65) 6533-6106
APACTraining@f5.com

F5 Networks, Inc.

Japan

Akasaka Garden City 19F
4-15-1 Akasaka, Minato-ku
Tokyo 107-0052 Japan
T (81) 3 5114-3200
F (81) 3 5114-3201
JapanTraining@f5.com

Legal Notices

Copyright

Copyright 2017; F5 Networks; Inc. All rights reserved.

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

Trademarks

AAM, Access Policy Manager, Advanced Client Authentication, Advanced Firewall Manager, Advanced Routing, AFM, APM, Application Acceleration Manager, Application Security Manager, AskF5, ASM, BIG-IP, BIG-IP EDGE GATEWAY, BIG-IQ, Cloud Extender, Cloud Manager, CloudFucious, Clustered Multiprocessing, CMP, COHESION, Data Manager, DDoS Frontline, DDoS SWAT, Defense.Net, defense.net [DESIGN], DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, ELEVATE, EM, ENGAGE, Enterprise Manager, F5, F5 [DESIGN], F5 Agility, F5 Certified [DESIGN], F5 Networks, F5 SalesXchange [DESIGN], F5 Synthesis, f5 Synthesis, F5 Synthesis [DESIGN], F5 TechXchange [DESIGN], Fast Application Proxy, Fast Cache, FCINCO, Global Traffic Manager, GTM, GUARDIAN, iApps, IBR, iCall, iControl, iHealth, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iQuery, iRules, iRules OnDemand, iSession, L7 Rate Shaping, LC, Link Controller, LineRate, LineRate Point, LineRate Precision, LineRate Systems [DESIGN], Local Traffic Manager, LROS, LTM, Message Security Manager, MobileSafe, MSM, OneConnect, Packet Velocity, PEM, Policy Enforcement Manager, Protocol Security Manager, PSM, Ready Defense, Real Traffic Policy Builder, SalesXchange, ScaleN, SDAS (except in Japan), SDC, Signalling Delivery Controller, Solutions for an application world, Software Designed Applications Services, Silverline, SSL Acceleration, SSL Everywhere, StrongBox, SuperVIP, SYN Check, SYNTHESIS, TCP Express, TDR, TechXchange, TMOS, TotALL, TDR, TMOS, Traffic Management Operating System, Traffix, Traffix [DESIGN], Transparent Data Reduction, UNITY, VAULT, vCMP, VE F5 [DESIGN], Versafe, Versafe [DESIGN], VIPRION, Virtual Clustered Multiprocessing, WebSafe, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent. All other product and company names herein may be trademarks of their respective owners.

Materials

The material reproduced on this manual; including but not limited to graphics; text; pictures; photographs; layout and the like ("Content"); are protected by United States Copyright law. Absolutely no Content from this manual may be copied; reproduced; exchanged; published; sold or distributed without the prior written consent of F5 Networks; Inc.

Patents

This product may be protected by one or more patents indicated at:

<http://www.f5.com/about/policies/patents>

Part One: High Availability and Traffic Processing

Table of Contents

Labs	1
Lab 1: Configuring High Availability	1
Lab 2: Managing Traffic Groups	10
Lab 3: Configuring Ratio (member) Load Balancing and Priority Group Activation	13
Lab 3A (Optional): Sync the Configuration	17

Part One: High Availability and Traffic Processing

Lab 1: Configuring High Availability



This lab corresponds with the activities presented in *Getting Started with LTM: Part 1 – Module 1 High Availability*, **Lesson Two: Setting Up an Active-Standby Pair**

Estimated time for completion: 20 minutes

Lab Objectives

- Use the Config Sync/HA Utility to configure High Availability (HA) settings, establish device trust, and create an active-standby device group
- Perform an initial ConfigSync operation to synchronize configuration data between the devices in a device group

Lab Requirements

You must have successfully completed the instructions entitled *Starting Up the Lab Environment* in the *Getting Started Lab Introduction* document.

Lab Introduction

In the lab environment, there are two BIG-IP systems. We will refer to bigip1.f5tn.com as “BIG-IP 1” and bigip2.f5tn.com as “BIG-IP 2”. Pay particular attention to the instructions. Some tasks will be performed on BIG-IP 1 and others on BIG-IP 2, which can be summarized as:

BIG-IP 2

1. Run Config Sync/HA Utility until you see the “Setup Utility Complete” confirmation message.

BIG-IP 1

2. Run Config Sync/HA Utility until you see the “Setup Utility Complete” confirmation message.
3. Establish device trust and configure a device group.
4. Perform initial sync called “ConfigSync”

Access the BIG-IP System

- Click the **Firefox web browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at <https://192.168.1.31>.)
- Log in to your BIG-IP system as the **admin** user and with password **admin**.

1. Once you have successfully logged into BIG-IP 1, open another browser by clicking the green + icon as indicated below:



2. In the browser, enter **https://192.168.2.31** to access BIG-IP 2.
3. When prompted, log in as **admin** with a password of **admin**.
4. You should have two browser tabs open side-by-side as indicated below:



Each system is ONLINE (ACTIVE) Standalone

Set Up BIG-IP 2

1. Begin with BIG-IP 2. Click the tab BIG-IP – bigip2.f5trn.com. We will refer to this as “BIG-IP 2.”
2. Scroll down and click on **Run Config Sync/HA Utility** link under the Setup Utility section.
3. Click the **Next** button under the **Standard Network Configuration** heading.
4. The **Redundant Device Wizard Options** is displayed. Click **Next**.

5. Confirm the settings and modify if necessary for VLAN **internal** as shown in the table below.

Internal Network Configuration section		
	Self IP	Address: 172.16.2.31 Netmask: 255.255.0.0 Port Lockdown: Allow Default
	Floating IP	Address: 172.16.2.33 Port Lockdown: Allow Default
Internal VLAN Configuration section		
	Interfaces	VLAN Interfaces: 1.2 (untagged)
When complete, click...	Next	

6. Confirm the settings and modify if necessary for VLAN **external** as shown in the table below.

External Network Configuration section		
	Self IP	Address: 10.10.2.31 Netmask: 255.255.0.0 Port Lockdown: Allow None
	Floating IP	Address: 10.10.2.33 Port Lockdown: Allow None
External VLAN Configuration section		
	Interfaces	Interfaces: 1.1 (untagged)
When complete, click...	Next	

7. Configure the high availability network to use the existing VLAN named **internal**.

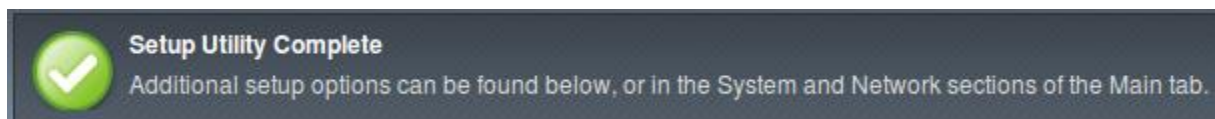
High Availability Network Configuration section	
High Availability VLAN	Click the Select existing VLAN radio button
Select VLAN	internal
When complete, click...	Next

8. The **Network Time Protocol Configuration** screen is displayed. Enter **172.16.20.1** and click **Add**. Click the **Next** button to continue.
9. The **Domain Name Server Configuration** screen is displayed. Click **Next**.
10. Confirm the **ConfigSync** settings on the non-floating Self IP for VLAN **internal** as in the table below.

ConfigSync Configuration section	
Local Address	172.16.2.31 (internal)
When complete, click...	Next

11. Accept the default settings for **Failover Unicast Configuration** and **Failover Multicast Configuration**. Click **Next**.
12. Accept the default primary and secondary local mirror address settings for **Mirroring Configuration**. Click **Next**.
13. Beneath the **Advanced Device Management Configuration**, click **Finished**.

You should see:



Congratulations! You're halfway there...

Set Up BIG-IP 1

Next, run the Config Sync /HA utility on BIG-IP 1 by following these steps:

14. Click the tab **BIG-IP – bigip1.f5trn.com**. We will refer to this as “BIG-IP 1”.



15. Scroll down and click on **Run Config Sync/HA Utility** link.
16. Click the **Next** button under the **Standard Network Configuration** heading.
17. The **Redundant Device Wizard Options** is displayed. Click **Next**.
18. Confirm the settings and modify if necessary for VLAN **internal** as shown in the table below.

Internal Network Configuration section		
	Self IP	Address: 172.16.1.31 Netmask: 255.255.0.0 Port Lockdown: Allow Default
	Floating IP	Address: 172.16.1.33 Port Lockdown: Allow Default
Internal VLAN Configuration section		
	Interfaces	VLAN Interfaces: 1.2 (untagged)
When complete, click...		Next

19. Confirm the settings and modify if necessary for VLAN **external** as shown in the table below.

External Network Configuration section		
Self IP	Address: 10.10.1.31 Netmask: 255.255.0.0 Port Lockdown: Allow None	
Default Gateway	Leave blank	
Floating IP	Address: 10.10.1.33 Port Lockdown: Allow None	
External VLAN Configuration section		
Interfaces	VLAN Interfaces: 1.1 (untagged)	
When complete, click...	Next	

20. Configure the high availability network to use the existing VLAN named **internal**.

High Availability Network Configuration section		
High Availability VLAN	Click the Select existing VLAN radio button	
Select VLAN	internal	
When complete, click...	Next	

21. The **Network Time Protocol Configuration** screen is displayed. Enter **172.16.20.1** and click **Add**. Click the **Next** button to continue.
22. The **Domain Name Server Configuration** screen is displayed. Click **Next**.

23. Configure ConfigSync on the non-floating self IP for VLAN **internal**, the VLAN we're using for high availability (HA).



ConfigSync Configuration section		
	Local Address	172.16.1.31 (internal)
When complete, click...	Next	

24. Accept the default settings for **Failover Unicast Configuration** and **Failover Multicast Configuration**. Click **Next**.
25. Accept the default primary and secondary local mirror address settings for **Mirroring Configuration**. Click **Next**.
26. In the **Standard Pair Configuration** section, click **Next**.
27. In the **Discover Configured Peer or Subordinate Device** section, click **Next**.
28. The **Retrieve Device Credentials** screen appears. Enter the configuration information according to the settings in the table below:

Retrieve Device Credentials (Step 1 of 3)		
	Device Type	Peer
	Device IP Address	192.168.2.31
	Administrator Username	admin
	Administrator Password	admin
When complete, click...		Retrieve Device Information
Verify Device Certificate (Step 2 of 3)		
	Verify that the information in the peer BIG-IP system device certificate is correct.	
When complete, click...		Device Certificate Matches
Add Device (Step 3 of 3)		
	Name	bigip2.f5trn.com
When complete, click...		Add Device

You should see the **Setup Utility Complete** message.

Toggle back and forth between the two BIG-IP systems.

One BIG-IP System will display:	The other BIG-IP system will display:
	

Synchronizing the Configuration from BIG-IP 1 to BIG-IP 2

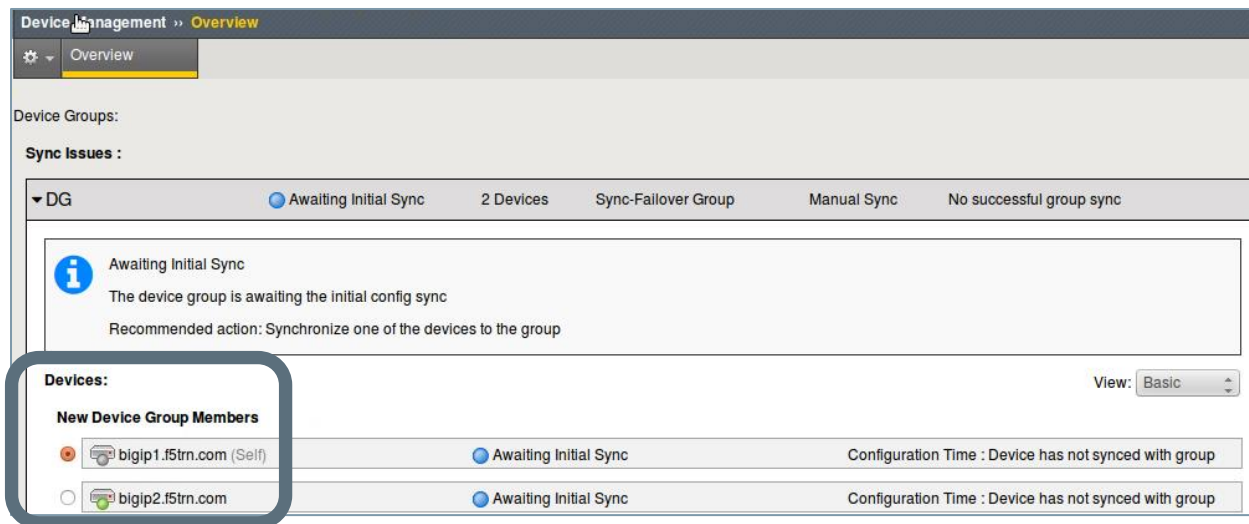


Synchronization should always be performed from the system with the desired configuration to the other device(s) in the device group. In this lab, we want to retain the configuration on BIGIP-1, so we will synchronize the configuration from BIGIP-1 to BIGIP-2.

29. Click on **BIG-IP 1**.

30. Click on the **Awaiting Initial Sync** link next to the red F5 icon.

31. This takes you to the **Device Management » Overview** screen as shown below:

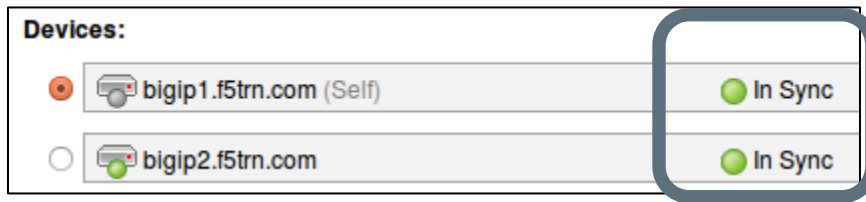


32. In the Devices section, notice the radio button is selected for **bigip1.f5trn.com (Self)**.

33. Under Sync Options, verify the radio button **Push the selected device configuration to the group** is selected.

34. Click the **Sync** button to initiate the ConfigSync.

After the sync is complete, the Sync Status should display two green circles to indicate that the two devices are in sync:



Toggle back and forth between the two BIG-IP systems.

One BIG-IP System will display:	The other BIG-IP system will display:
<p>The screenshot shows the BIG-IP logo, a vertical bar, and the text 'ONLINE (STANDBY)' and 'In Sync'.</p>	<p>The screenshot shows the BIG-IP logo, a vertical bar, and the text 'ONLINE (ACTIVE)' and 'In Sync'.</p>

You may have to log back into BIG-IP 2.



You may continue with Lab 2, or end your lab session now.

Lab 2: Managing Traffic Groups



This lab corresponds with the activities presented in *Getting Started with LTM: Part 1 – Module 2 Traffic Processing*, **Lesson Three: Managing Traffic Groups**

Estimated time for completion: 10 minutes

Lab Objectives

- Force a traffic group from the active device to the standby device
- Verify functionality

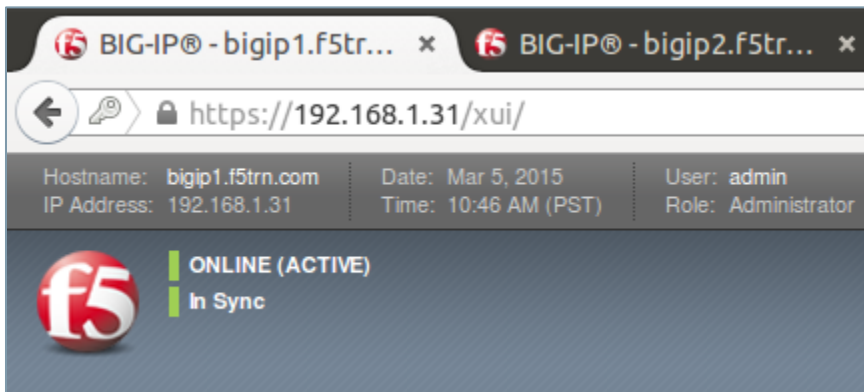
Lab Requirements

- Student must complete Lab 1 prior to beginning Lab 2.
- Continue to Step 1 on the next page.

1. If you have not already done so, log into BIG-IP1 and open another browser by clicking the green + icon as indicated below:



2. In the browser, enter **https://192.168.2.31** to access BIG-IP 2.
3. When prompted, log in as **admin** with a password of **admin**.
4. You should have two browser tabs open side-by-side as indicated below:



One system is ONLINE (ACTIVE) In Sync and the other is ONLINE (STANDBY) In Sync

View Traffic Group Failover Objects

5. Click on the **Active** system and navigate to **Device Management » Traffic Groups**.

Expected Results

- You should see the Status is ACTIVE.
The Next Active Device is the other BIG-IP system.

6. Click on **traffic-group-1**.
7. Click on the **Failover Objects** tab.

Expected Results

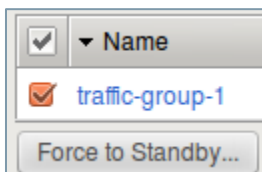
- You should see the two floating IP Addresses. The floating self IPs were created when you ran the Config Sync/HA Utility.
- If we had Virtual Servers configured at this time, the Virtual Addresses would be listed along with the self IP addresses.

Failover the Active Traffic Group

Let's suppose you want to do maintenance on the Active BIG-IP system without impacting application delivery. You can manually float a traffic group from the current Active Device to the Next Active Device using the Force to Standby button. You can only perform this task from the device that is Active for this traffic group.

8. From the **Active** system, navigate to **Device Management » Traffic Groups**.

9. Click the check box next to traffic-group-1 as indicated below:



10. Click **Force to Standby**.

11. Click **Force to Standby** again to confirm.

12. Toggle back and forth between the two BIG-IP systems. Navigate to **Device Management » Traffic Groups** on each system.

One BIG-IP System will display:	The other BIG-IP system will display:																
<table border="1"> <thead> <tr> <th colspan="2">Failover Status</th></tr> </thead> <tbody> <tr> <td>Status</td><td>ACTIVE</td></tr> <tr> <td>Summary</td><td>1/1 active</td></tr> <tr> <td>Details</td><td></td></tr> </tbody> </table>	Failover Status		Status	ACTIVE	Summary	1/1 active	Details		<table border="1"> <thead> <tr> <th colspan="2">Failover Status</th></tr> </thead> <tbody> <tr> <td>Status</td><td>STANDBY</td></tr> <tr> <td>Summary</td><td>1/1 standby</td></tr> <tr> <td>Details</td><td></td></tr> </tbody> </table>	Failover Status		Status	STANDBY	Summary	1/1 standby	Details	
Failover Status																	
Status	ACTIVE																
Summary	1/1 active																
Details																	
Failover Status																	
Status	STANDBY																
Summary	1/1 standby																
Details																	

Expected Results

- You have forced traffic-group-1 to become standby on this device
- Click on the other BIG-IP, and it will be Active for traffic-group-1
- When toggling between the two systems, one BIG-IP system will be active for traffic-group-1, and the other system will be standby for traffic-group-1.



You may continue with Lab 3, or end your lab session now.

Lab 3: Configuring Ratio (member) Load Balancing and Priority Group Activation



This lab corresponds with the activities presented in *Getting Started with LTM: Part 1 – Module 2 Traffic Processing, Lesson One: Load Balancing*

Estimated time for completion: 20 minutes

Lab Objectives

- Configure a pool to load balance traffic with Ratio (member) load balancing method
- Configure a priority group for each pool member
- Configure Priority Activation by specifying a minimum threshold number for members that must be available for load balancing
- Test Priority Activation by disabling a pool member
- Verify functionality via statistics

Lab Requirements

You must have successfully completed the instructions entitled “Starting up the Lab Environment” in the *Getting Started Lab Introduction* document.

Access the BIG-IP System

- If you have not done so already, click the **Firefox Web Browser** icon in the toolbar to access your BIG-IP system. (The icon automatically opens a browser session to the BIG-IP system at <https://192.168.1.31>.)
- If you are continuing from Lab 2: Managing Traffic Groups, make sure to access the **Active** BIG-IP system for this lab.
- Log in to your BIG-IP system as the **admin** user and with password **admin**.
- Continue with Step 1 on the next page.

Create a Pool

1. Create a ratio (member) load balancing pool with Priority Group Activation using the information in the following table.

Configuration utility		
Local Traffic » Pools » Pool List , then click Create		
Configuration section		
	Configuration	Basic
	Name	http_pool
	Health Monitors	http
Resource section:		
	Load Balancing Method	Ratio (member)
	Priority Group Activation	Less than...
	Available Member(s)	2
	New Members	Address: 172.16.20.1
		Service Port: 80
		Ratio: 5
		Priority: 10 and click Add
		Address: 172.16.20.2
		Service Port: 80
		Ratio: 5
		Priority: 10 and click Add
		Address: 172.16.20.3
		Service Port: 80
		Ratio: 1
		Priority: 5 and click Add
When complete, click...		Finished

Create a Virtual Server

2. Create a Virtual Server that uses the pool created in the previous step.

Configuration utility		
Local Traffic » Virtual Servers » Virtual Server List, then click Create		
General Properties section		
Name	http_vs	
Type:	Standard	
Destination Address:	10.10.1.100	
Service Port	80 (or type or select HTTP)	
State	Enabled	
Resources section:		
Default Pool	http_pool	
When complete, click...	Finished	

3. Open a new browser session and connect to **http://10.10.1.100**.
4. Refresh the screen 5-10 times by pressing **Ctrl-F5**.
5. From the **Active** BIG-IP system, navigate to **Statistics » Module Statistics: Local Traffic**.
6. From the **Statistics Type** menu, select **Pools**. Was the traffic sent to pool member 172.16.20.3? Why or why not? _____
7. Select the checkbox to the left of http_pool and click the **Reset** button to clear statistics.
8. Navigate to **Local Traffic » Pools** and click **http_pool**.
9. Click the **Members** tab.
10. Select the **checkbox** next to **172.16.20.2:80** and click **Disable**.
11. Connect to **http://10.10.1.100** and refresh the screen 5-10 times by pressing **Ctrl-F5**.
12. View the pool statistics again. Was traffic sent to pool member 172.16.20.3? What configuration setting allowed traffic to this pool member? _____
13. **Enable** pool member **172.16.20.2**.
14. **Reset** the statistics for **http_pool**.
15. Connect to **http://10.10.1.100** and refresh the screen 5-10 times by pressing **Ctrl-F5**.
16. **Refresh** and view the pool statistics. What are the results? _____

Expected Results

- Initially, you should see traffic for pool members 172.16.20.1 and 172.16.20.2, and you should see no traffic for pool member 172.16.20.3 because the Priority Group Activation setting is set to a minimum of two pool members available.
- After disabling pool member 172.16.20.2, you should see traffic to 172.16.20.1 and 172.16.20.3, and you should see no traffic for the disabled pool member 172.16.20.2. Recall that Priority Group Activation for this pool requires that at least two pool members are active.
- Once you enable pool member 172.16.20.2, you should see traffic for pool members 172.16.20.1 and 172.16.20.2, and you should see no traffic for pool member 172.16.20.3



If you have continued from Lab 1 and Lab 2 and you have an Active-Standby pair of BIG-IPs, you may continue with Optional Lab 3A. If not, end your lab session now.

Optional Lab 3A: Sync the Configuration



This lab corresponds with the activities presented in *Getting Started with LTM: Part 1 – Module 2 Traffic Processing, Lesson Two: Synchronizing Configuration Data*

1. On each of the BIG-IP systems, navigate to **Local Traffic » Network Map**. One system should display the virtual server and pool you created. The other system should be empty and display “Local Traffic Network Map and No Objects found”.
2. Click on the **ONLINE (ACTIVE)** BIG-IP system.



Synchronizing the Configuration from the Active BIGIP system to the Standby BIGIP system

3. Click the **Changes Pending** link next to the red f5 icon.
4. This takes you to the **Device Management » Overview** section.
5. In the **Devices** section, below Recent Changes, verify the radio button for **bigip1.f5trn.com (Self)** is selected.
6. Under the Sync options, verify **Push the selected device configuration to the group** radio button is selected.
7. Click the **Sync** button to initiate the ConfigSync.

The Sync Status should display two green circles to indicate that the two devices are in sync:

Devices:	
<input checked="" type="radio"/>  bigip1.f5trn.com (Self)	 In Sync
<input type="radio"/>  bigip2.f5trn.com	 In Sync

8. Toggle back and forth between the two BIG-IP systems.

One BIG-IP System will display:	The other BIG-IP system will display:
 ONLINE (STANDBY) In Sync	 ONLINE (ACTIVE) In Sync

9. On each of the BIG-IP systems, navigate to **Local Traffic » Network Map**. Both systems should display the virtual server and pool you created in the previous lab.



You have completed the labs associated with this WBT. Please terminate your lab session now.