F5 Training

MODULE - 1

INTRODUCTION

INTRODUCTION

- Load Balancer, as the name suggests is a tool which balances load. Since we are dealing with networks, it basically does “Network Load Balancing”. Now, if I had to define “Load Balancing”, I would preferably do it as, *“Load balancing (performed by a load balancer) is a type of service performed by a tool that assigns work loads to a set of servers in such a manner that the computing resources are used in an optimal manner”*. This optimal manner may be any thing and it is configurable.
- Load balancers are used to increase

Types of SLB

Load balancers are generally grouped into two categories:

- **Layer 7** : It load balancers distribute requests based upon data found in application layer protocols such as HTTP.
- **Layer 4** : Layer 4 load balancers act upon data found in network and transport layer protocols (IP, TCP, FTP, UDP).

IS LOAD BALANCING DIFFERENT FROM CLUSTERING?

- Load-Balancing and Clustering are both solutions to the same problem but they go about it somewhat differently. Clustering usually refers to the use of proprietary software to interact at an OS level and is specific to the vendor in question.
- Since there is a requirement for tight integration between servers, special software is required, and thus the vendor will only support a finite amount of platforms. Typically, the cost of the network application device is the same if not less than the "clustering" software solution.
- Additionally, there is less to trouble-shoot with the Load-Balancer than there is with their software counterparts. Similarly, scalability is usually much easier to achieve with a Load-Balancer as all the user must do is add a

LB Vendor Comparison

Vendor	Device	L4 CPS	L4 Throughput (Gbps)	L7 CPS	L7 RPS	SSL TPS (2K Key)	SSL Bulk Throughput (Gbps)	Compression (Gbps)
F5	VIPRION 2400 chassis with (1) B2100 blade.	400,000	40	150,000	1,000,000	10,000	9	10.0
F5	BIG-IP 4200v	300,000	10	100,000	850,000	9,000	8	8.0
Cisco	ACE 30 Blade	500,000	8	200,000	*	*	6	6.0
Citrix	NetScaler MPX-11500	*	8	*	1,200,000	15,000	6	3.5
Radware	Alteon 5224XL	480,000	8	190,000	*	11,200	4.1	3.6

** We were unable to find numbers published by the vendor for these categories*

F5 Solutions

F5 products address the three main areas of Application Delivery Networking:

- Application security
- Application Optimization
- Application Availability

F5 Solution

BIG-IP LTM Features

Application Traffic Management

- Intelligent load balancing
- Application protocol support (HTTP/2, SSL/TLS, SIP, etc.)
- Application health monitoring
- Application connection state management
- F5 OneConnect
- Advanced routing (BGP, RIP, OSPF, ISIS, BFD)
- SDN services (VXLAN, NVGRE)

Application Delivery Optimization

- Symmetric adaptive compression
- RAM cache and compression
- TCP Express
- HTTP/2 gateway

Secure Application Delivery

- SSL connection and session mirroring
- Hybrid crypto services (Hardware SSL offload for BIG-IP VE)
- SSL/TLS encryption offload (hardware accelerated)
- Algorithm agility (GCM, ECC, Camellia, DSA, RSA)
- Suite B support including forward secrecy
- Internal/Network/Cloud HSM (FIPS 140-2)
- SSL visibility

Application Visibility and Monitoring

- F5 Analytics
- Performance dashboard
- High-speed logging
- sFlow

Programmable Infrastructure

- iRules and iRules LX for data plane programmability
- iCall for event-based control-plane scripting
- iApps for app-level config management and deployment
- iControl for Management API (SOAP, REST)

ScaleN

- On-demand scaling
- All-active application clustering
- Operational scaling (multi-tenant and virtualization)

MODULE - 2

BIG-IP LTM Platforms

What is BIG-IP Local Traffic Manager?

- ***BIG-IP® Local Traffic Manager*** controls network traffic that comes into or goes out of a local area network (LAN), including an intranet.
  - Local Traffic Manager includes a variety of features that perform functions such as inspecting and transforming header and content data, managing SSL certificate-based authentication, and compressing HTTP responses.
  - In so doing, the BIG-IP system not only directs traffic to the appropriate server resource, but also enhances network security and frees up server resources by

Deployment Modes

BIG-IP iSeries Appliances

VIPRION Chassis

BIG-IP Virtual Editions

BIG-IP Hardware Line-up

Price

BIG-IP 2000s

2000s

Dual core CPU
8 Gigaport +2 10Gig
1x 500GB HD
8 GB memory
SSL @ 2K TPS / 4 Gb Bulk
2.5 Gbps max software compression

5 Gbps Traffic

BIG-IP 5000s

1 quad core Intel Xeon processor
4 Gig+ 8 10Gig ports
1 TB HD
32 GB memory
SSL @ 10K TPS / 12 Gb bulk
6 Gbps max software compression

30 Gbps Traffic

BIG-IP 7050

1 quad core Intel Xeon processor
4 gig + 8 10Gigport
400 GB SSD
32 GB memory
SSL @ 15K TPS / 18 Gb bulk
9 Gbps max hardware compression

40-20 Gbps Traffic(l4/l7)

BIG-IP 10000

1 Intel hex core
16 110gig + 2x 40GB
2x 1TB drives (Raid1)
48 GB memory
SSL @ 21K TPS / 22 Gb bulk
12 Gbps max hardware compression

80/40 Gbps Traffic (l4/l7)

Function / Performance

Virtual Edition

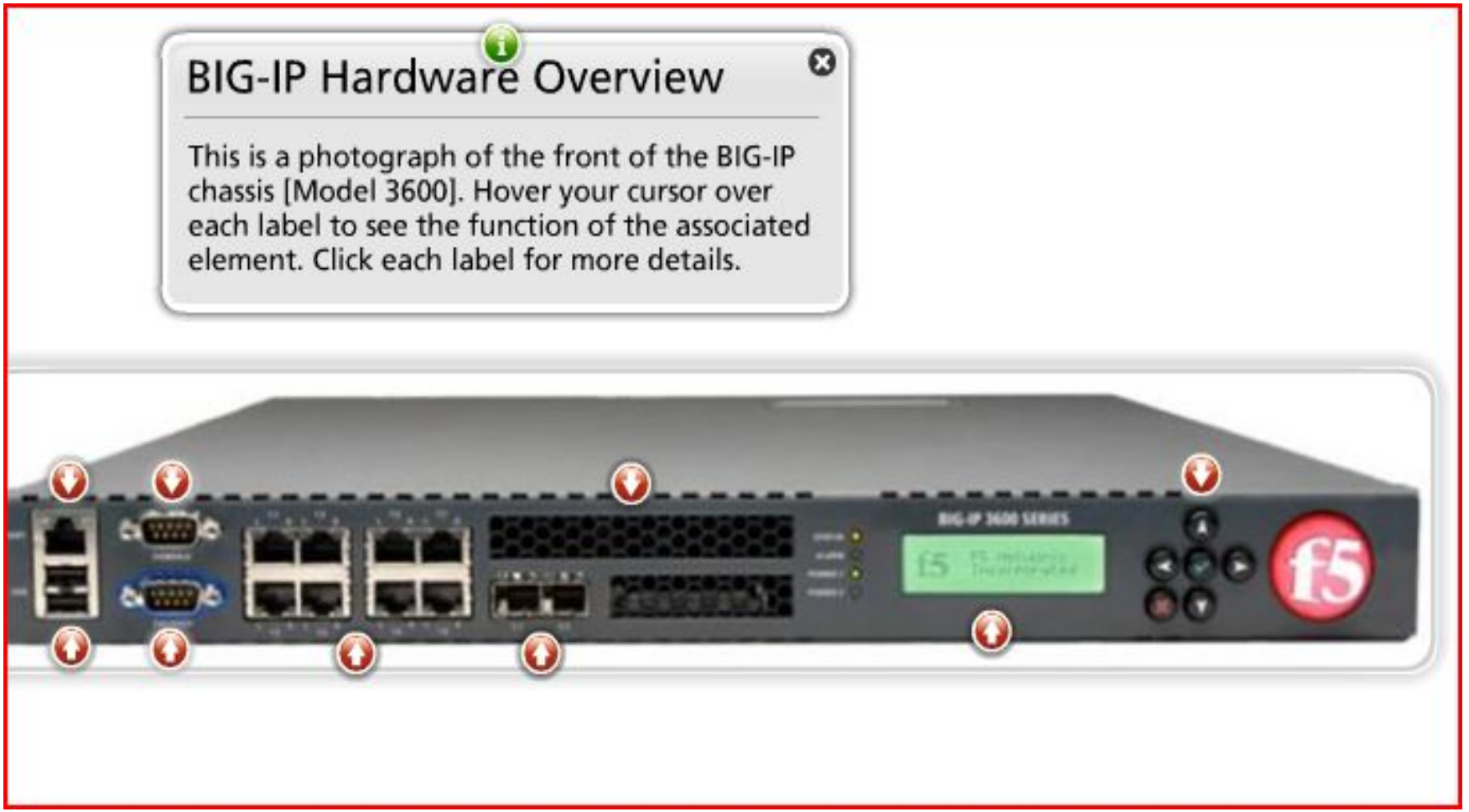
- F5® BIG-IP® virtual editions (VEs) are virtual application delivery controllers (vADCs) that can be deployed on all leading hypervisors and cloud platforms running on commodity servers.
- BIG-IP VEs deliver all the same market-leading application delivery services—including advanced traffic management, acceleration, DNS, firewall, and access management—that run on F5 purpose-built hardware.
- VE software images are downloadable and portable between on-premises virtualized data center, public cloud, and private cloud environments.

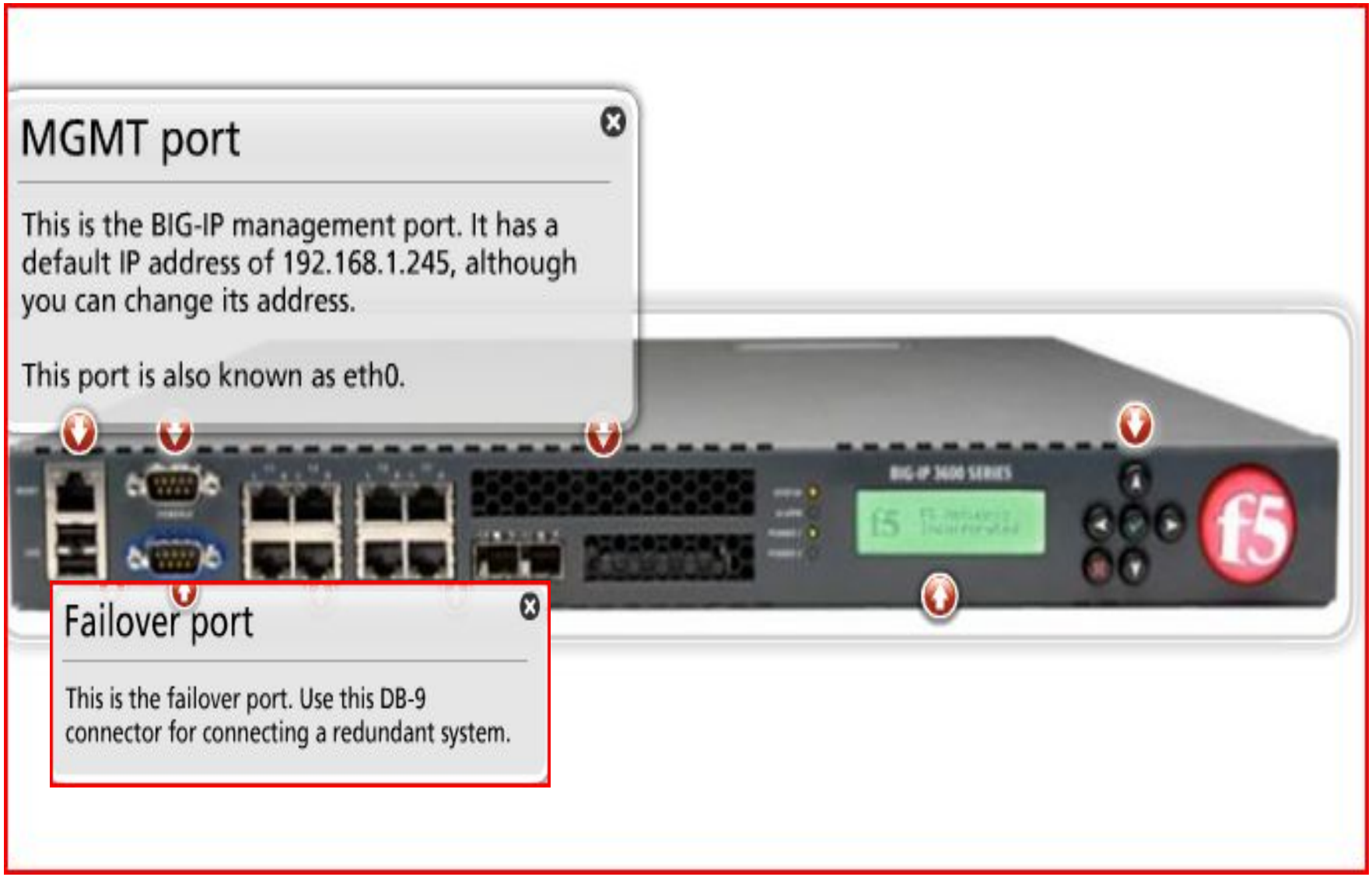
Download the free BIG-IP VE trial
Start testing how you can make your application fast, secure, and available with a full-featured BIG-IP VE—including BIG-IQ Centralized Management—in the environment of your choice. Download a 30-day trial of a BIG-IP VE now. Please review the "Getting Started" documentation

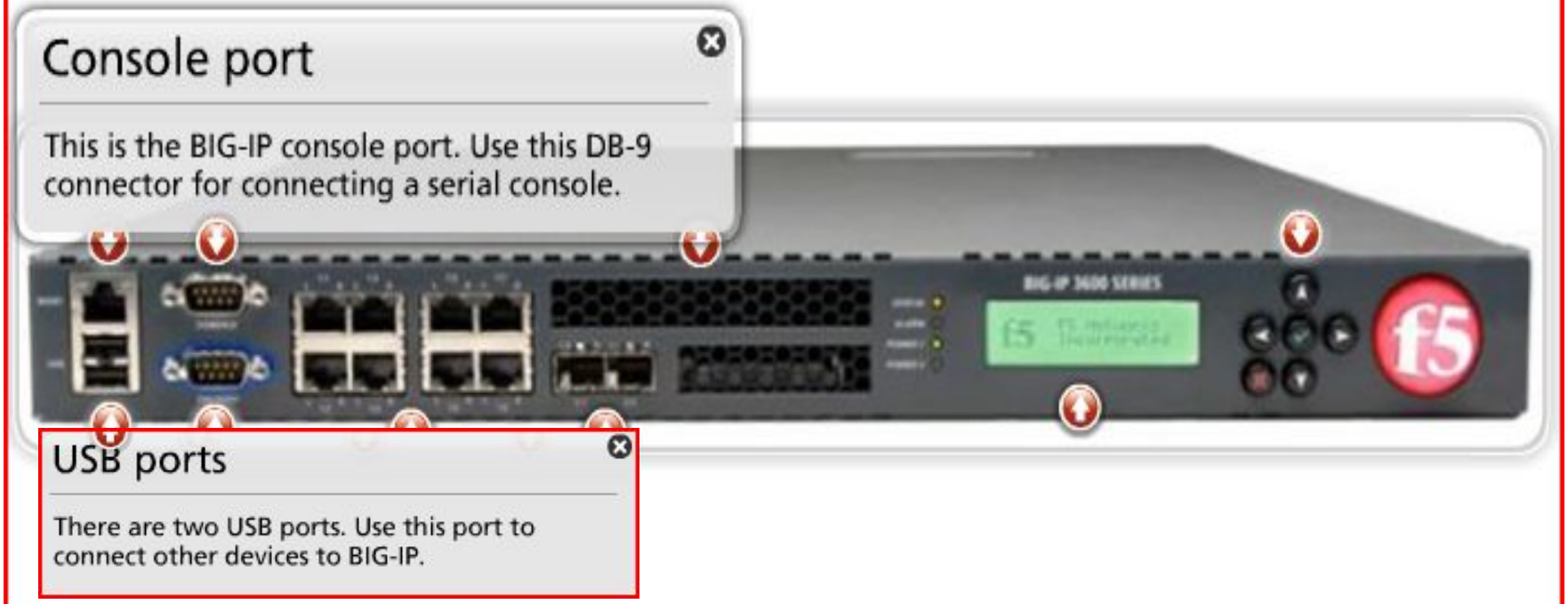
Viprion

- Each F5® VIPRION® platform is a single, powerful Application Delivery Controller (ADC) with modular performance blades you can add or remove without disrupting users or applications.
- Features:
- On-demand scaling improves performance
- Hardware DDoS approach mitigates attacks
- Blade options enable superior performance and security
- Operational scaling enables consolidation

Exploring Big-IP Hardware




MGMT port
This is the BIG-IP management port. It has a default IP address of 192.168.1.245, although you can change its address.
This port is also known as eth0.
Failover port
This is the failover port. Use this DB-9 connector for connecting a redundant system.
BIG-IP 3600 SERIES
f5


Console port
This is the BIG-IP console port. Use this DB-9 connector for connecting a serial console.
USB ports
There are two USB ports. Use this port to connect other devices to BIG-IP.
BIG-IP 3600 SERIES
f5

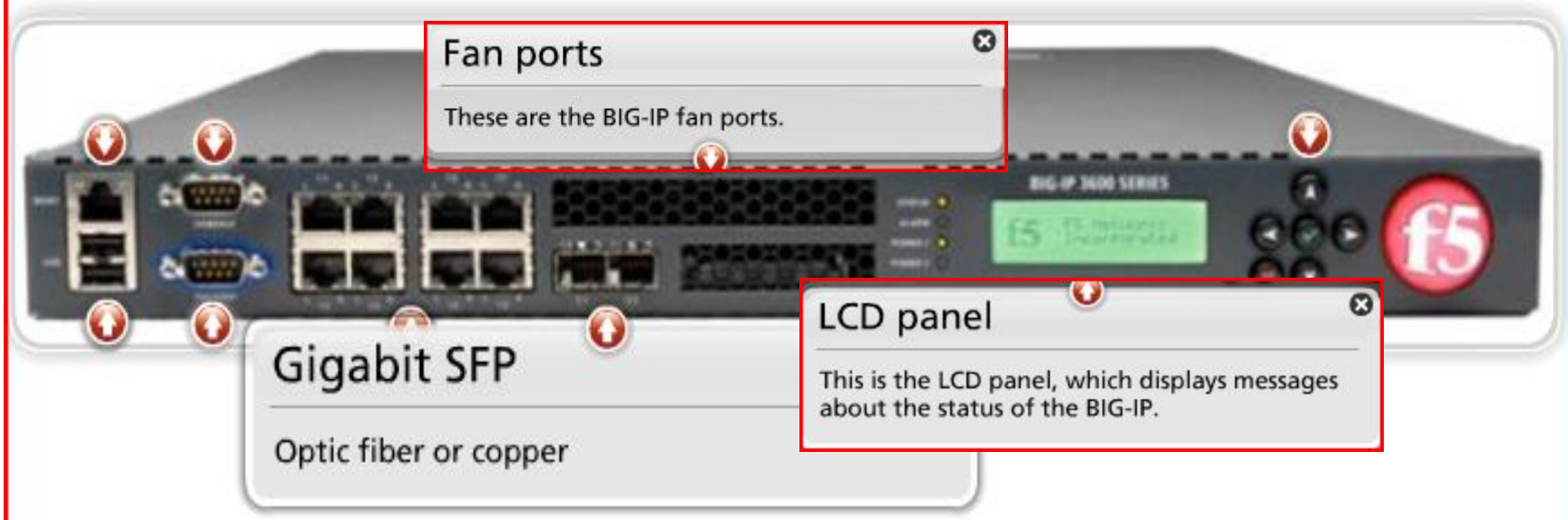
Controls for the LCD panel

These are the controls for the LCD panel. Using these controls, you can configure a number of BIG-IP settings.

Ethernet ports

Use these Ethernet ports to connect the BIG-IP to the network as well as to connect both clients and servers to the BIG-IP.

The Ethernet ports are numbered top to bottom and left to right. For example, the top left port is 1.1 while the port below it is 1.2.

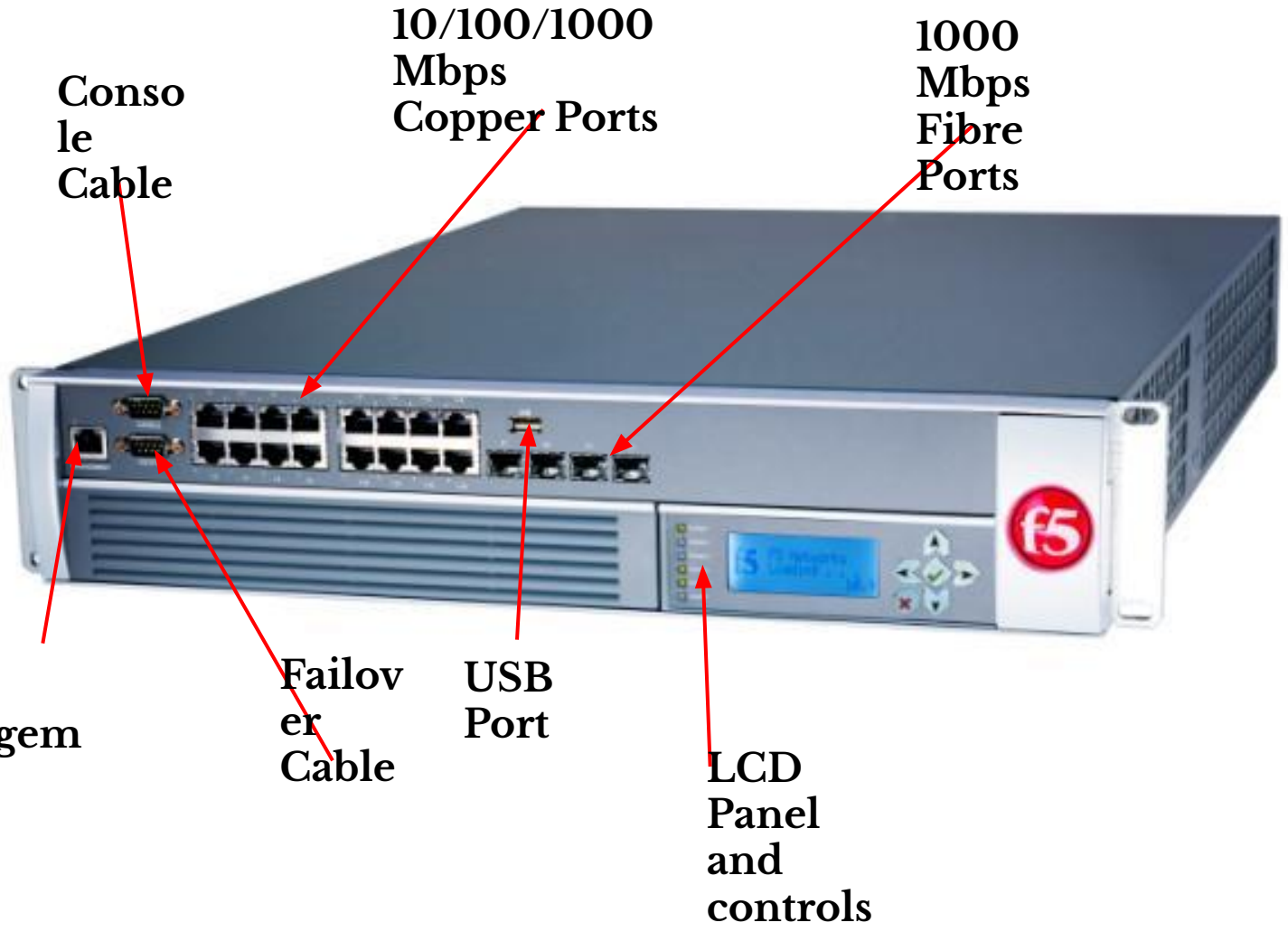

Fan ports
These are the BIG-IP fan ports.
LCD panel
This is the LCD panel, which displays messages about the status of the BIG-IP.
Gigabit SFP
Optic fiber or copper

MODULE 2

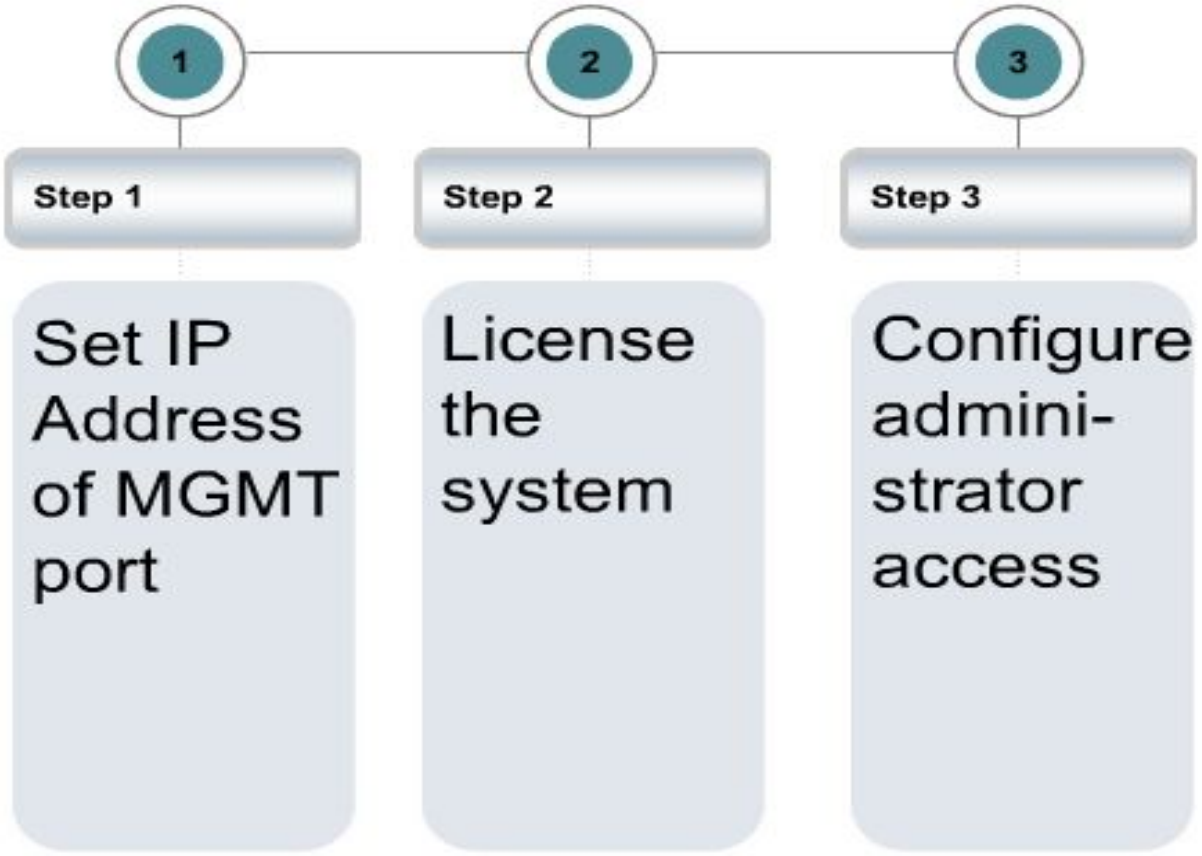
Initial Setup

- ☐ ***Exploring Big-IP Hardware***
- ☐ ***Exploring Big-IP File System***
- ☐ ***Licensing Big-IP***
- ☐ ***Basic Configuration***

The Hardware

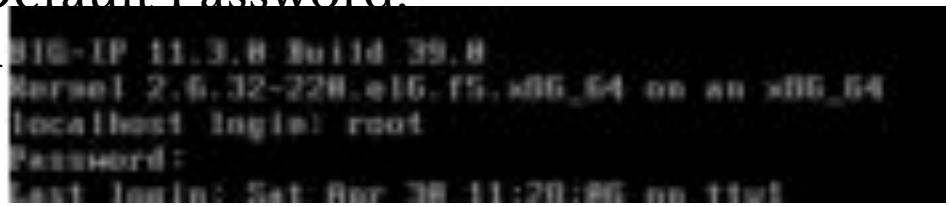


Setup Overview



Installat
ion:

Default
username: root
Default Password:
d



Enter the TMOS shell then issue the syntax found below to assign the IP address to management interface

```
[root@localhost:NO
LICENSE:Standalone] config # tmsh
```

```
root@(localhost)(cfg-sync Standalone)(NO LICENSE)(/Common)(tmos)# create
sys management-ip 192.168.99.51/255.255.255.0
```

the management's default gateway is optional depending on the setup.

```
root@(localhost)(cfg-sync Standalone)(NO LICENSE)(/Common)(tmos)#
create sys management-route default gateway 192.168.99.1
```

Display the

```
root@(localhost)(cfg-sync Standalone)(NO
LICENSE)(/Common)(tmos)# list sys management-route sys
management-route default { gateway 192.168.99.1 network
default }
```

```
root@(localhost)(cfg-sync Standalone)(NO
LICENSE)(/Common)(tmos)# list sys management-ip sys
management-ip 192.168.99.51/24 { description
configured-statically }
```

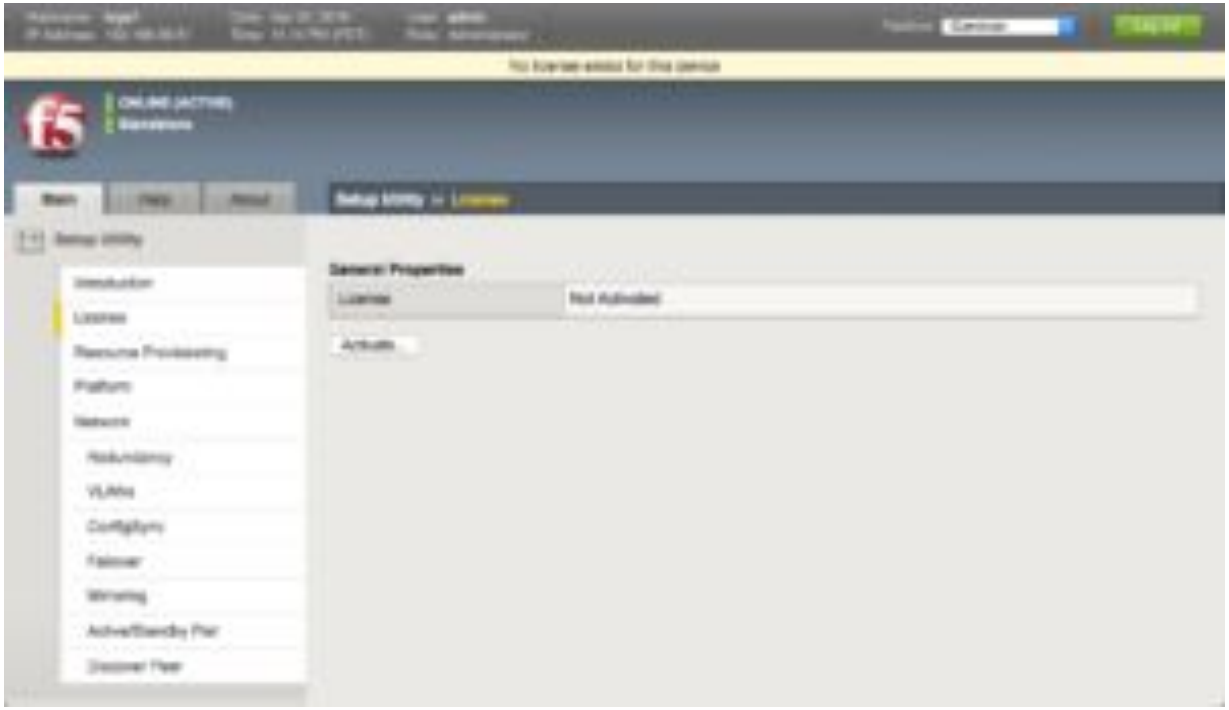
Save the configuration and browse the portal.

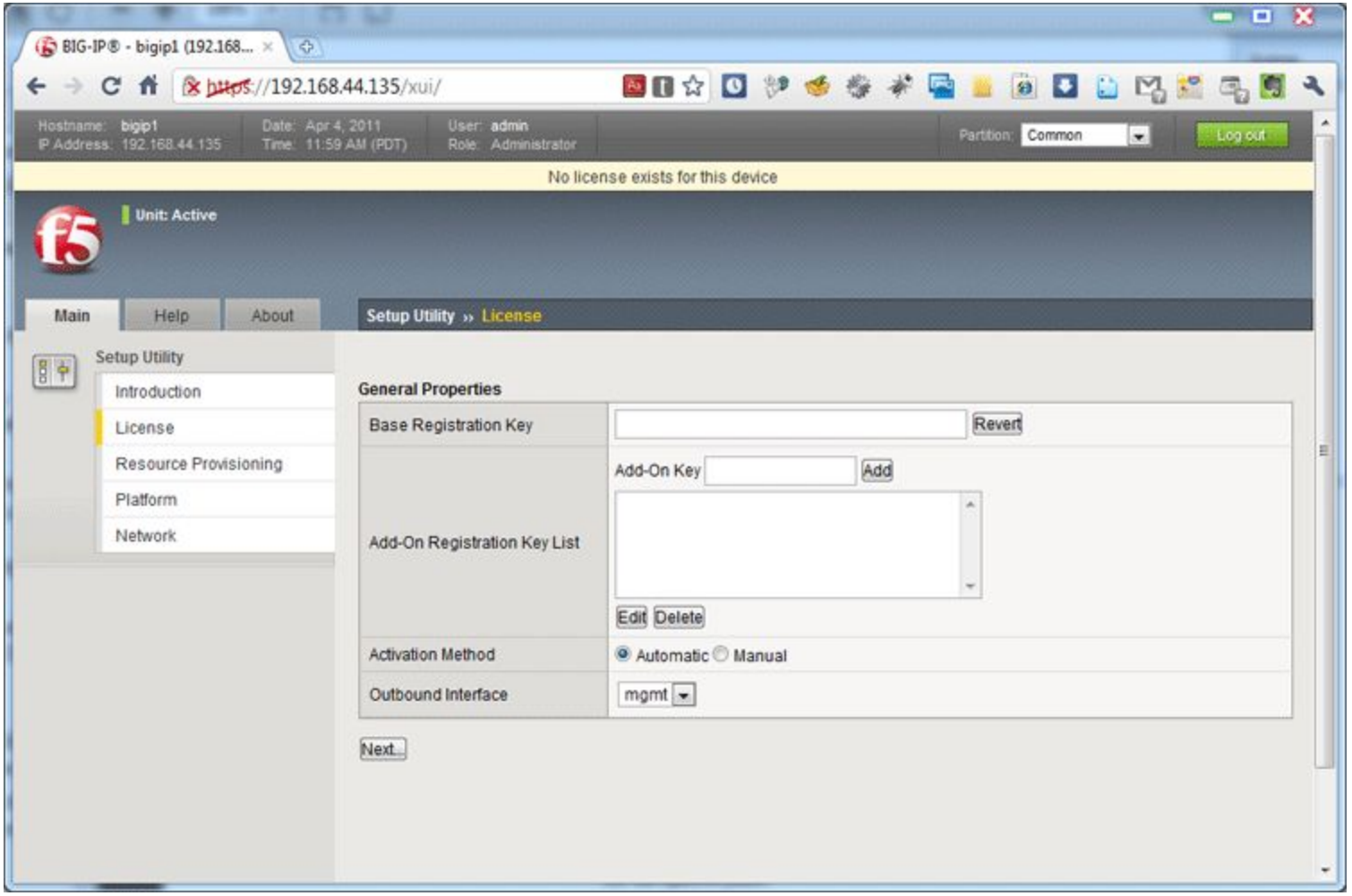
```
root@(localhost)(cfg-sync Standalone)(NO LICENSE)(/Common)(tmos)# save sys
config

Saving running configuration... /config/bigip.conf /config/bigip_base.conf
/config/bigip_user.conf
```

To access the BIG-IP Configuration Utility, open your favorite web browser and enter **https://BIG-IP mgmt address** here in the address bar. You will then be presented with a screen just like below. To log in, use the default username and password, which is **admin/admin**

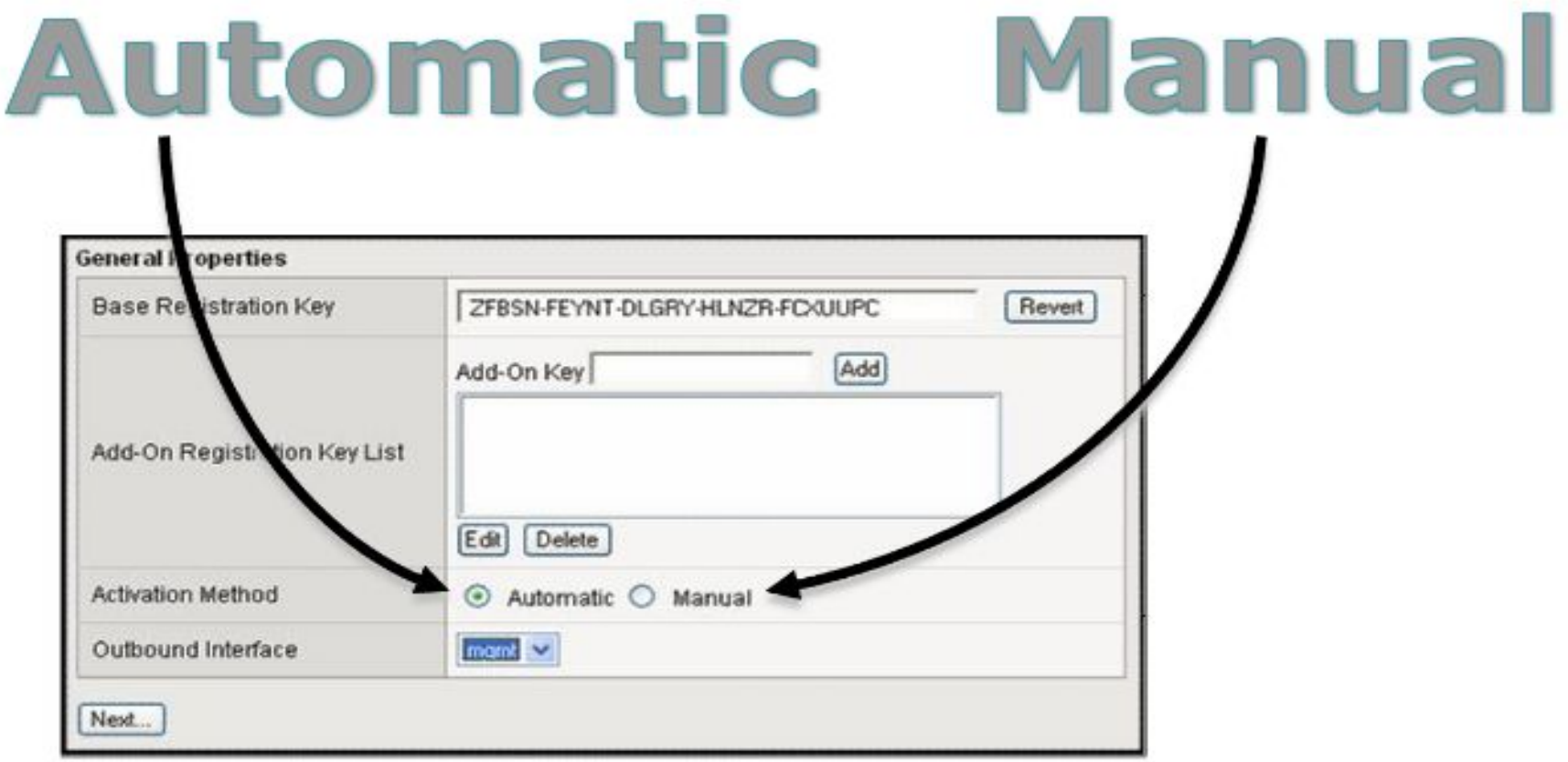
Once logged in, you will be presented with the Welcome screen. To begin the Setup Utility wizard, click Next to continue

You will now be presented with a screen that shows you to activate the BIG-IP LTM license. Click Activate.



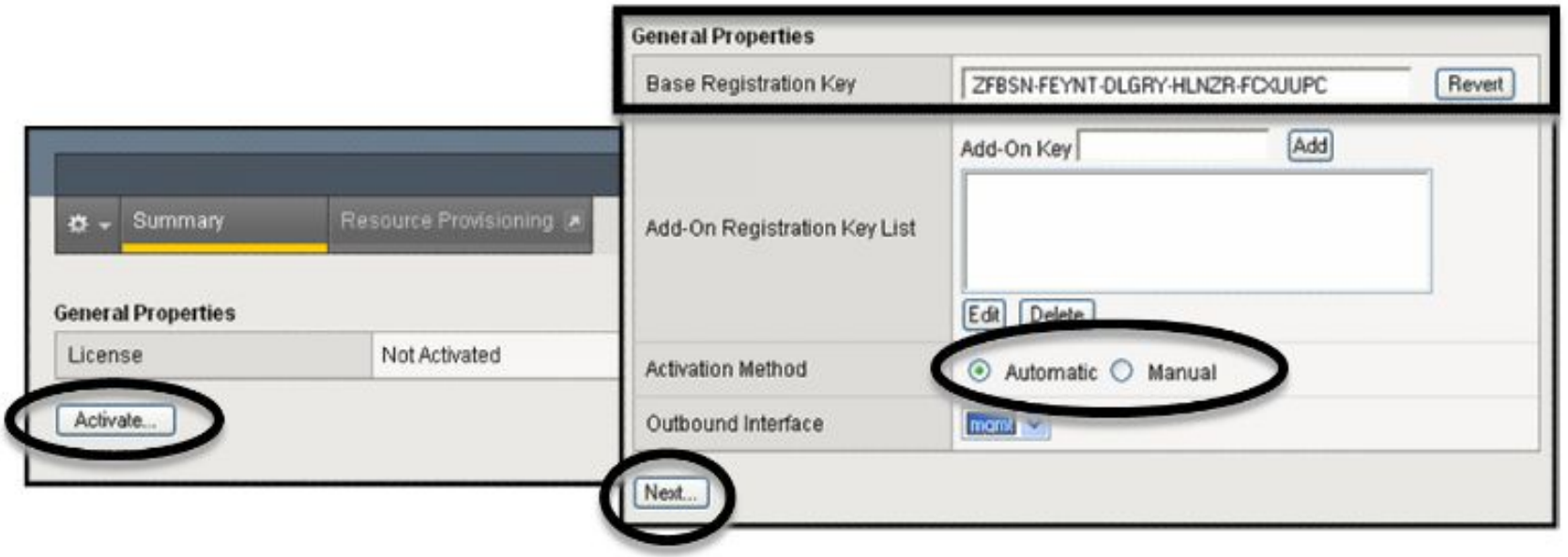

BIG-IP® - bigip1 (192.168...
https://192.168.44.135/xui/
Hostname: bigip1
IP Address: 192.168.44.135
Date: Apr 4, 2011
Time: 11:59 AM (PDT)
User: admin
Role: Administrator
Partition: Common
Log out
No license exists for this device
Unit: Active
Main
Help
About
Setup Utility ›› License
Setup Utility
Introduction
License
Resource Provisioning
Platform
Network
General Properties
Base Registration Key
Revert
Add-On Key
Add
Add-On Registration Key List
Edit
Delete
Activation Method
Automatic
Manual
Outbound Interface
mgmt
Next

Licensing Methods

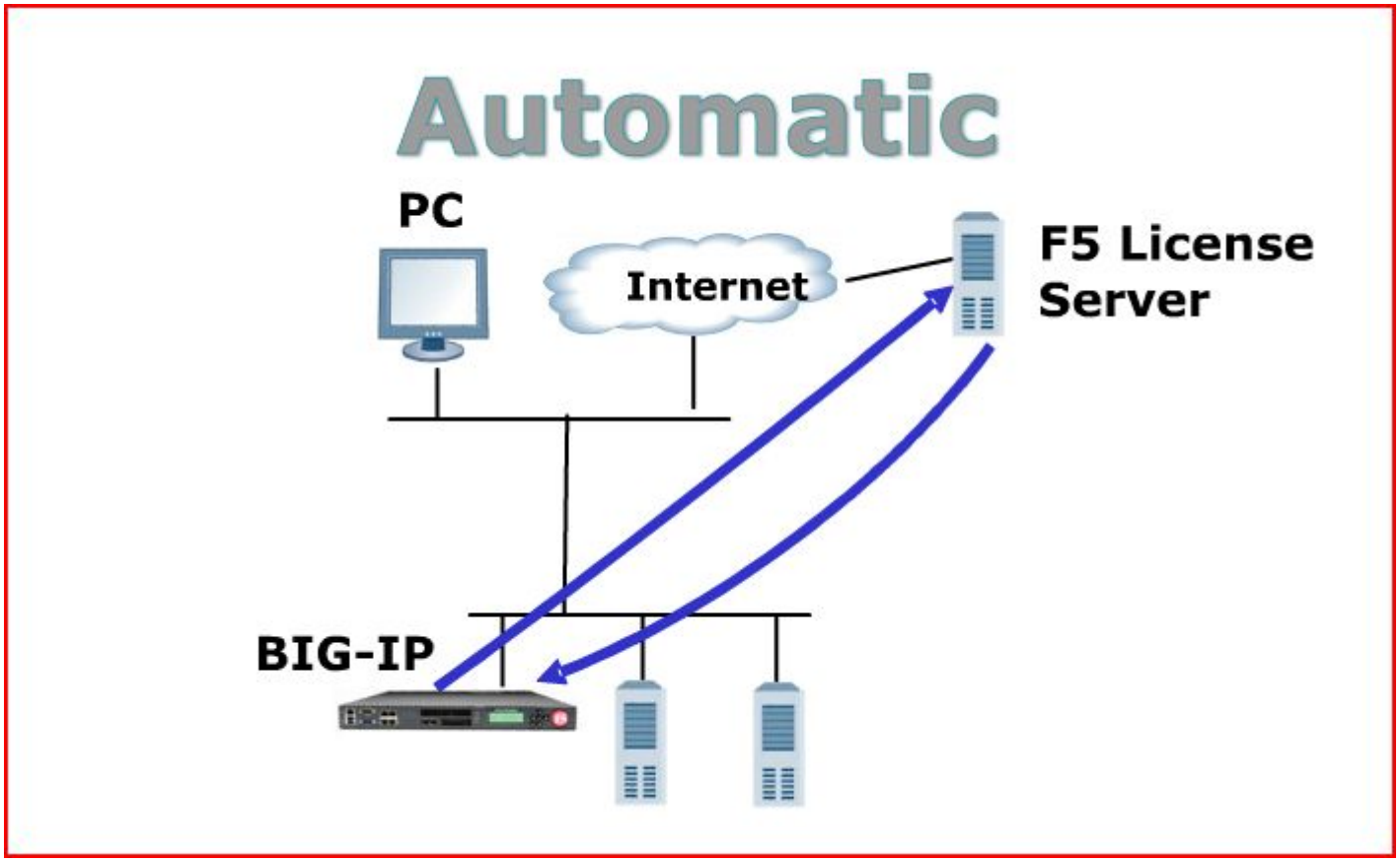


Entering Registration Key

1. Click **Activate**.
2. Enter your registration key.
3. Select **Automatic** or **Manual**.
4. Click **Next**.



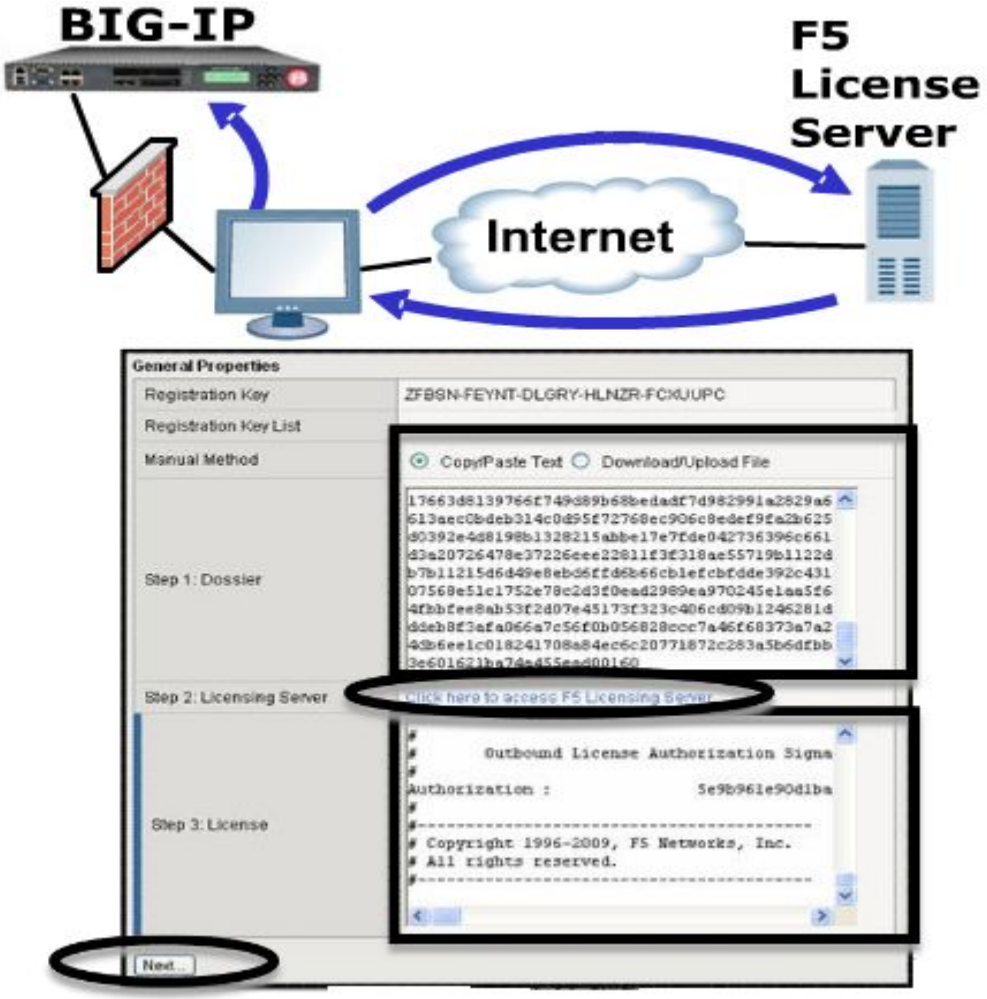
› Automatic Licensing



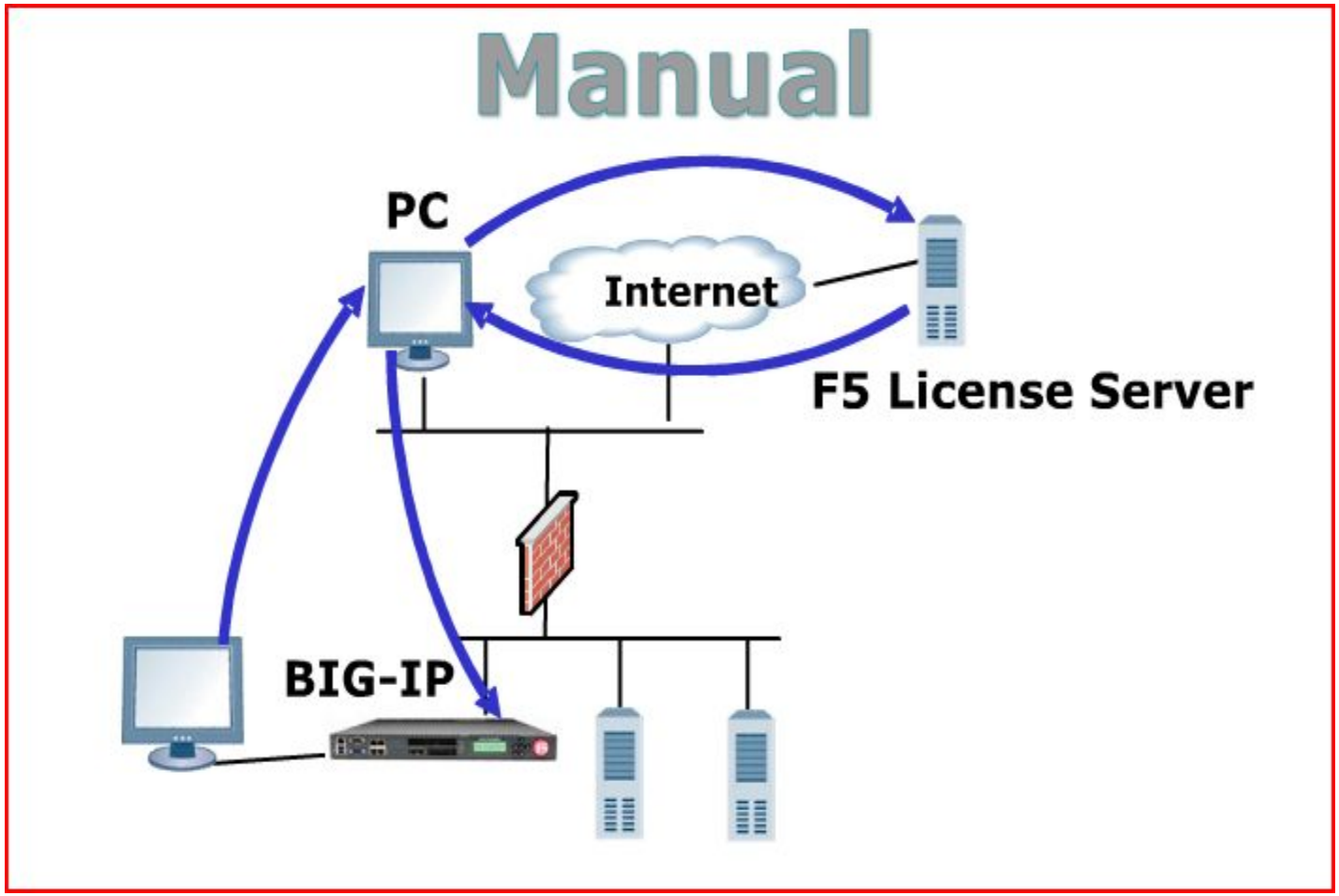
Manual Licensing

1. Copy dossier locally.
2. Connect PC to Internet.
3. Send dossier to F5 License Server.

   http://activate.f5.com
4. Get License from F5
5. Copy License to BIG-IP System
6. Click Next.

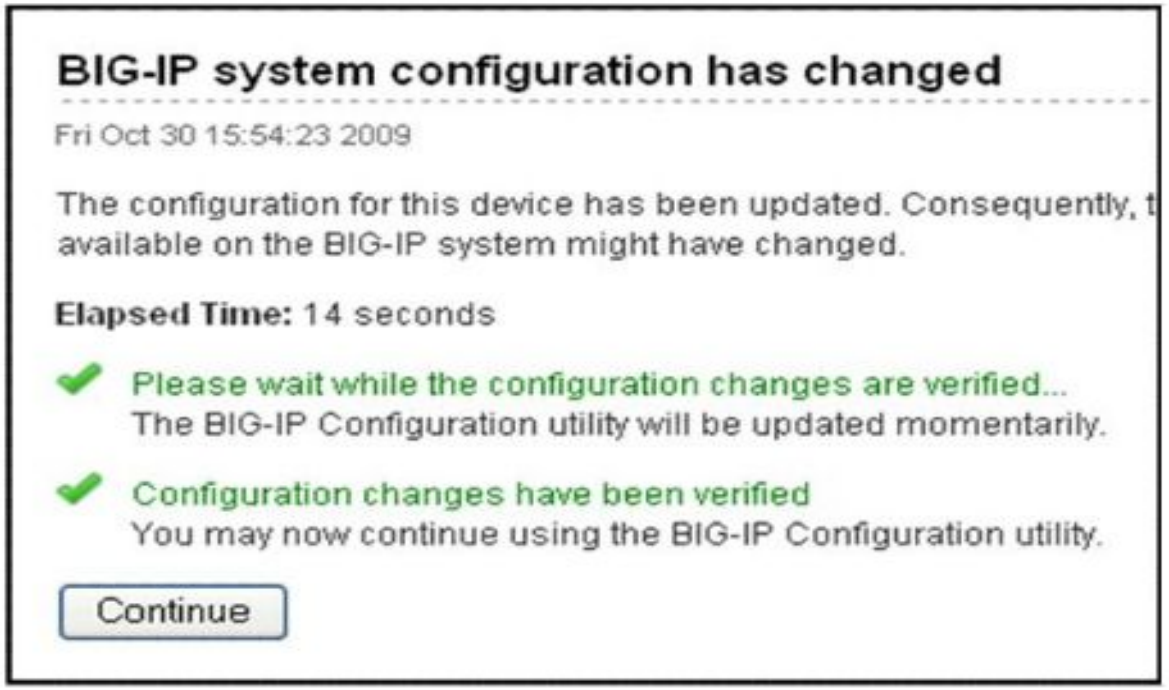


› Manual Licensing

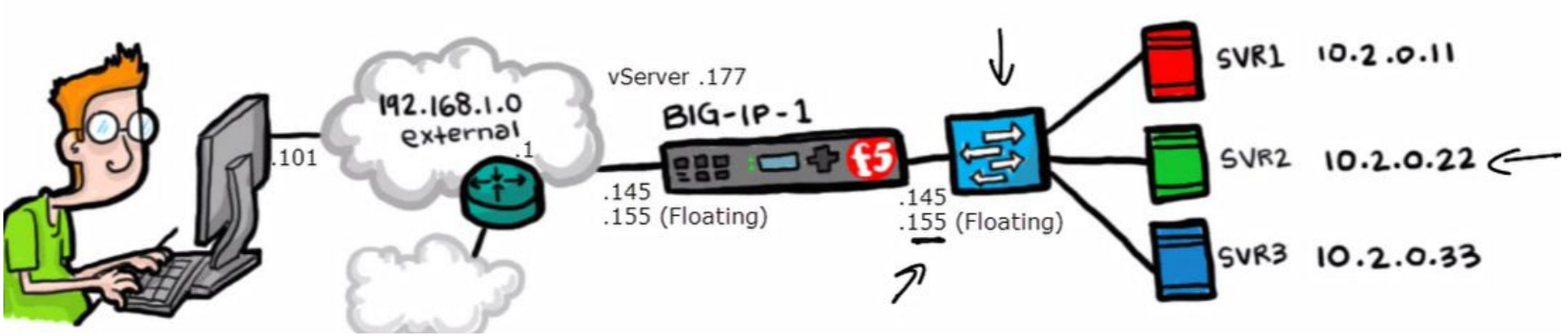


Completing the Licensing Process

1. Look for **Activation Complete** message.
2. Reboot BIG-IP.



Reference Topology



MODULE 3

LTM Terminology

Local traffic objects

The most basic objects in Local Traffic Manager that you must configure for local traffic management are:

- **Virtual Server**:

These acts like a virtual server with an Virtual IP, as the name suggests, this IP is not real and this is the IP on which client sends their requests. These servers receive the request from a client and then forward it directly to a “pool” or to a “I-Rule” which in turn forwards to a pool

- **Pools**:

This is a collection of Nodes (Actual Servers/ Computers), It may have 1 to N number of real nodes

Local traffic objects

- **Nodes:**

These are nothing but the actual IP address of the real servers which actually have to service the requests.

- **I-Rules (Or some times just "Rules"):**

They basically define the rules, which has to be met in order to get the requests serviced by the actual servers, in other words they control requests from reaching the actual servers based on some rules like source IP and the destination port. Normally they are associated with a pool as a destination and they are called by the Virtual servers

Local traffic objects

- **Health Monitors**:

Health Monitors are normally Keep a lives which are sent to the nodes in order to determine that they are healthy and can process data. For Example, A web server should accept connections at port 80, if it doesn't then it is probably down and cannot service the requests, we have different type of health monitors and these are determined by the server we are using and the port we want to connect.

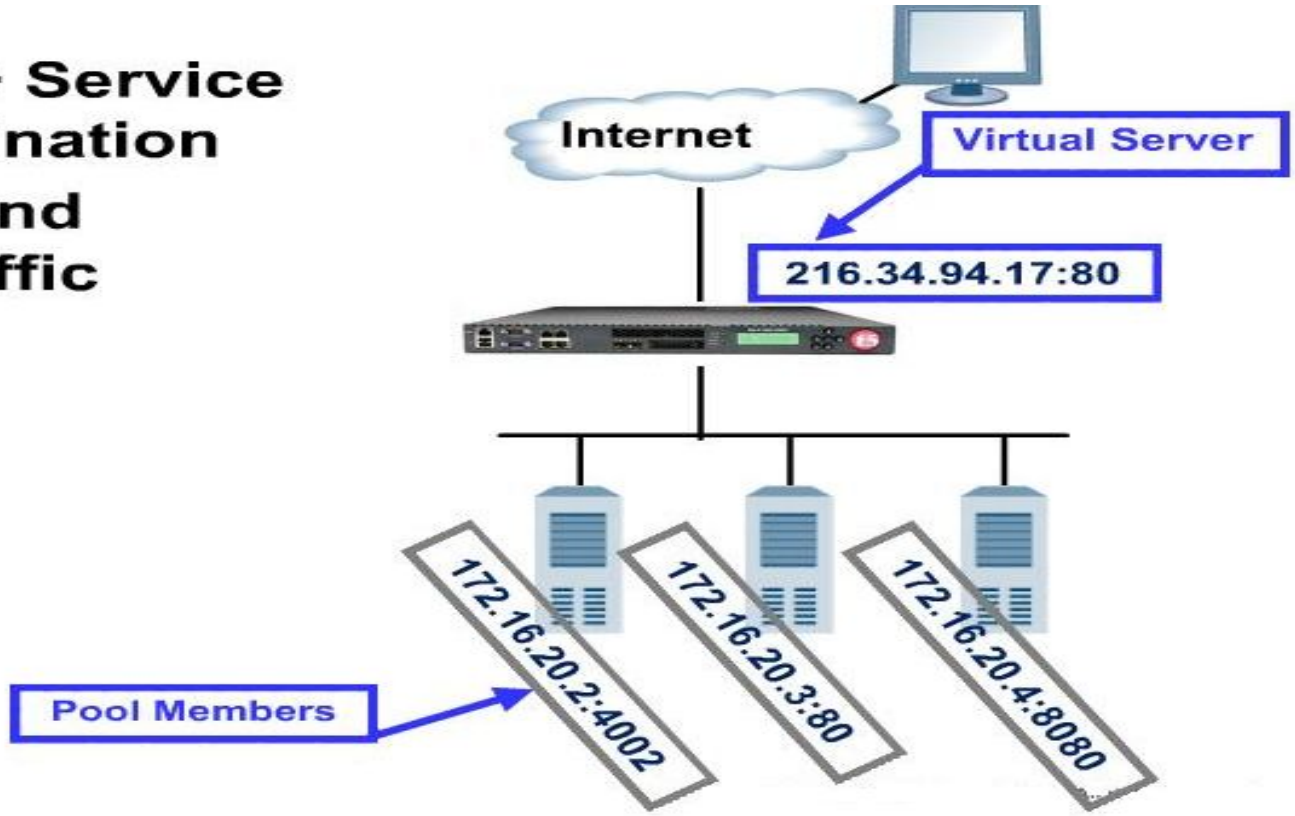
Virtual Server

-Big-IP is default deny device, so listener (virtual) is must

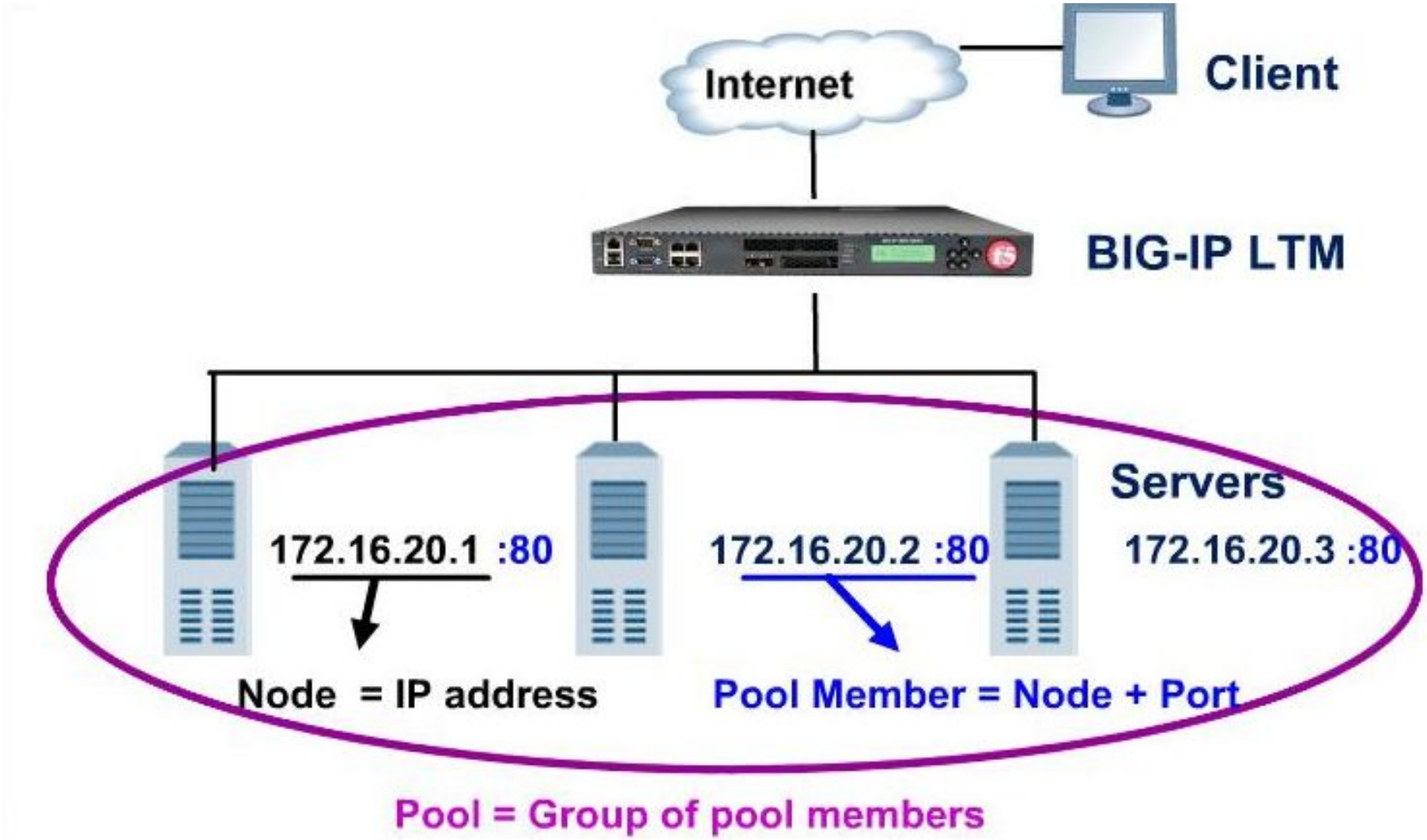
-Virtual server glues everything together

-Typically virtual are associated with pool

- **IP Address + Service (Port) Combination**
- ***Listens* for and manages traffic**



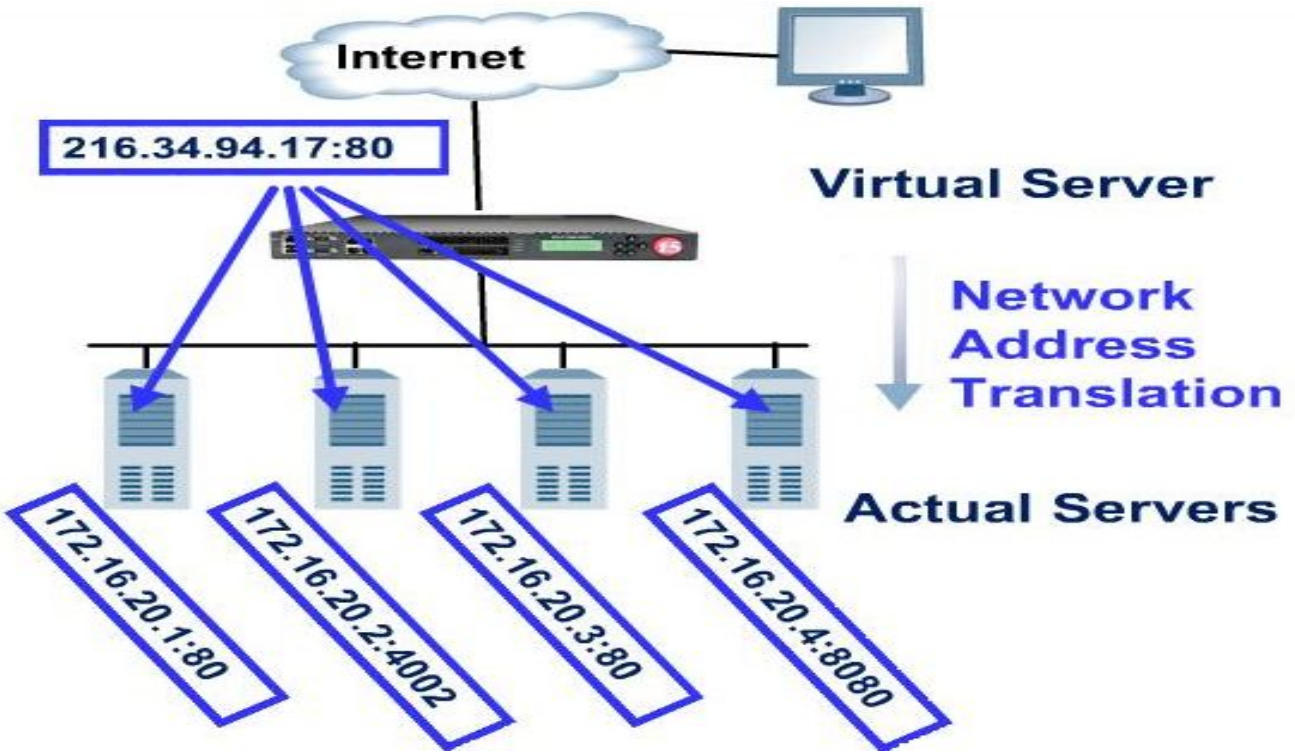
Pools , Members & Nodes



-Before virtual server can load balance it should mapped to pool

-Big-IP translate the destination ip address from virtual server to actual server

-Client see the pool servers as single server, hence the term Virtual Server

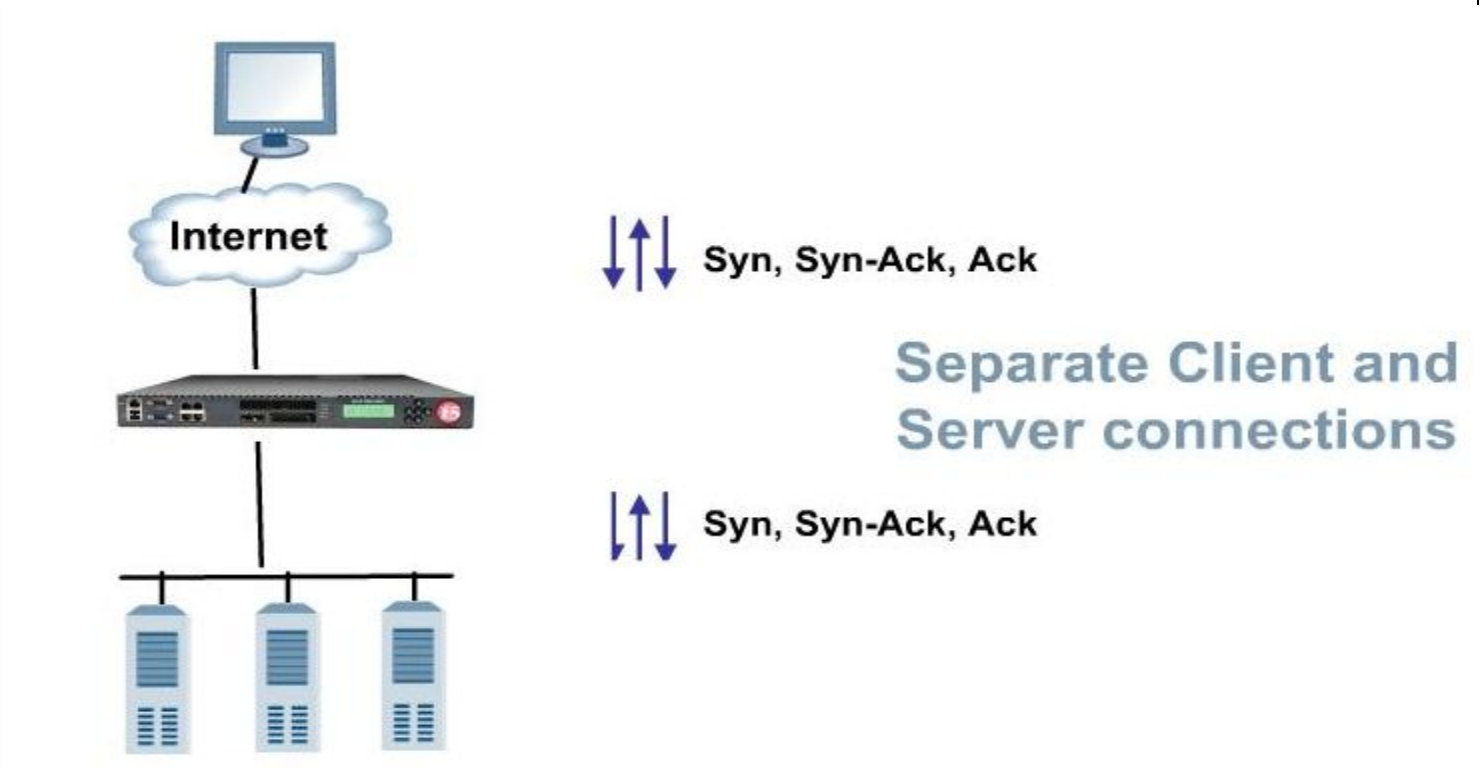


Full Proxy Architecture

-Big-IP do much more than translating the network Address

-F5 implemented full proxy architecture in Big-IP

-Separate tcp connections for the client & the server



Types of VIP

- Standard
  - Most common type of VIP for general purpose load balancing
  - Can make use of all functions including iRules, WebAccelerator, ASM etc
- Forwarding (Layer 2)
  - Generally used when LTM is configured in a bridge mode (VLAN Groups)
  - Essentially just forwards packets at Layer 2
- Forwarding (IP)
  - Used when LTM needs to forward or route packets
  - Can either just route them based on it's IP routing table of load balance multiple routers/firewalls etc
- Performance (HTTP)
  - Used for very simple, very fast HTTP load balancing
  - Loose a number of features (see next slide)
- Performance (Layer 4)
  - Used for general purpose fast load balancing of packets using the PVA ASIC
  - Loose a number of features depending on PVA Acceleration mode (see next few slides)

MODULE 4

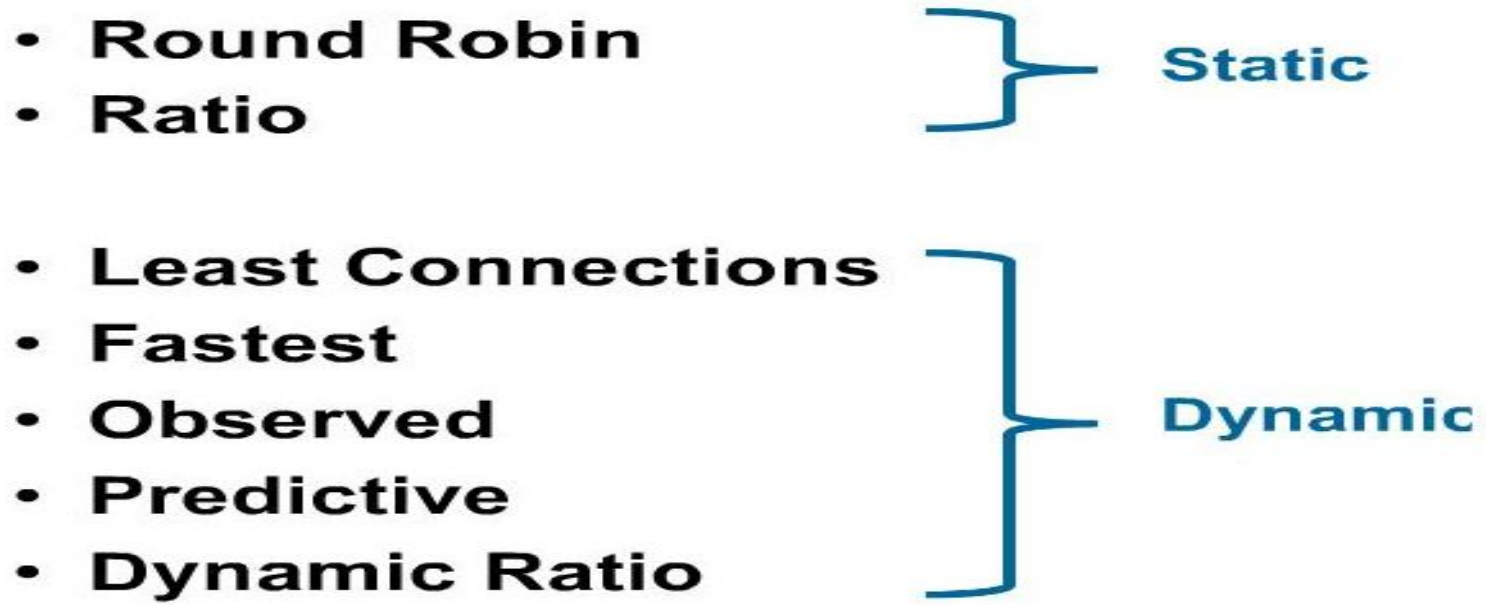
Load Balancing

- ***Load Balancing Method***
- ***Member vs Node***
- ***Priority Group Activation***
- ***Configuring load balancing***

Load Balancing Methods

-Static method do not take server performance in to consideration

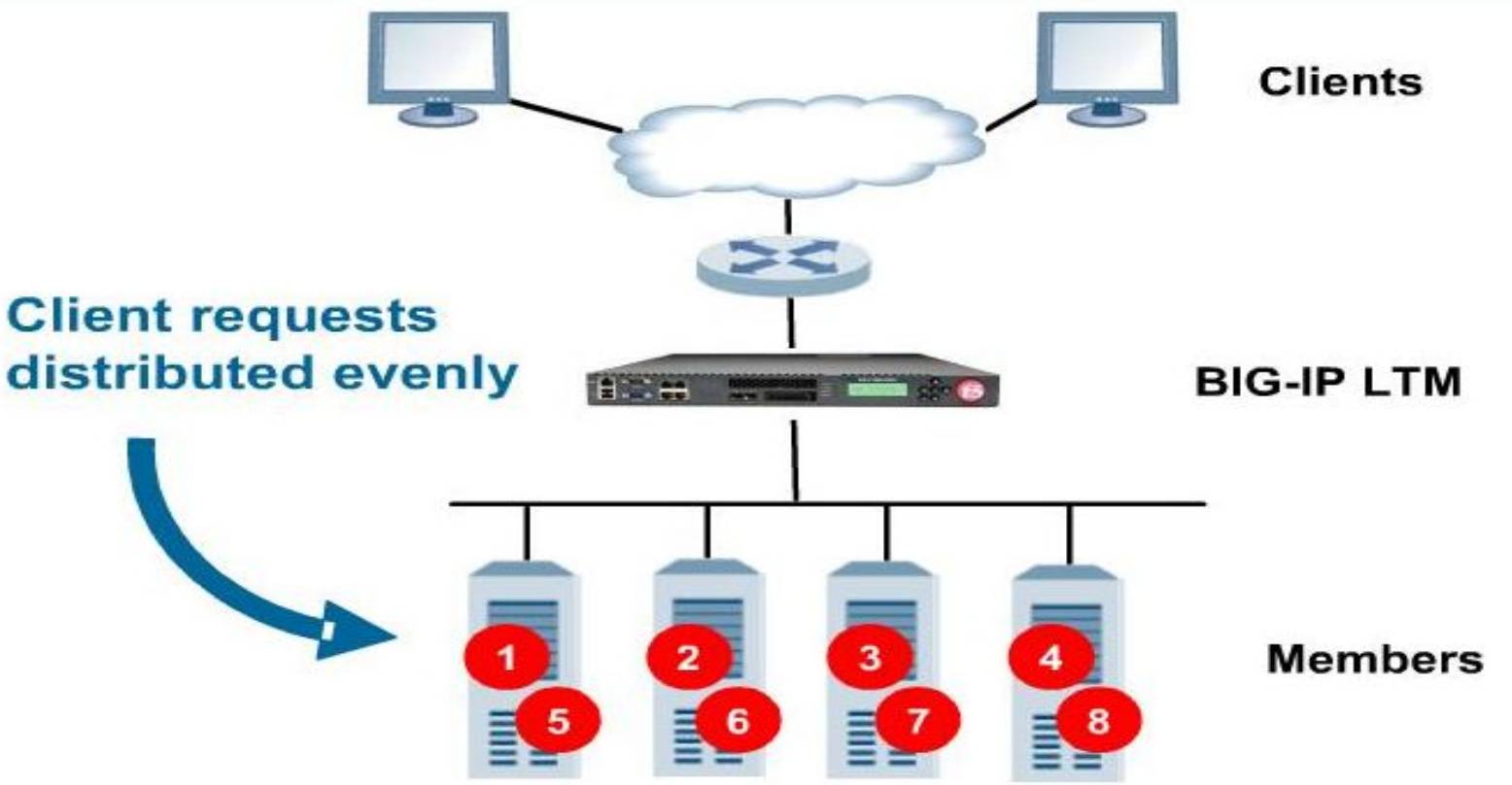
-Dynamic method does consider server performance



Round Robin

-Round Robin is default & most commonly used method

-Big-IP evenly distributes client request across all available pool member



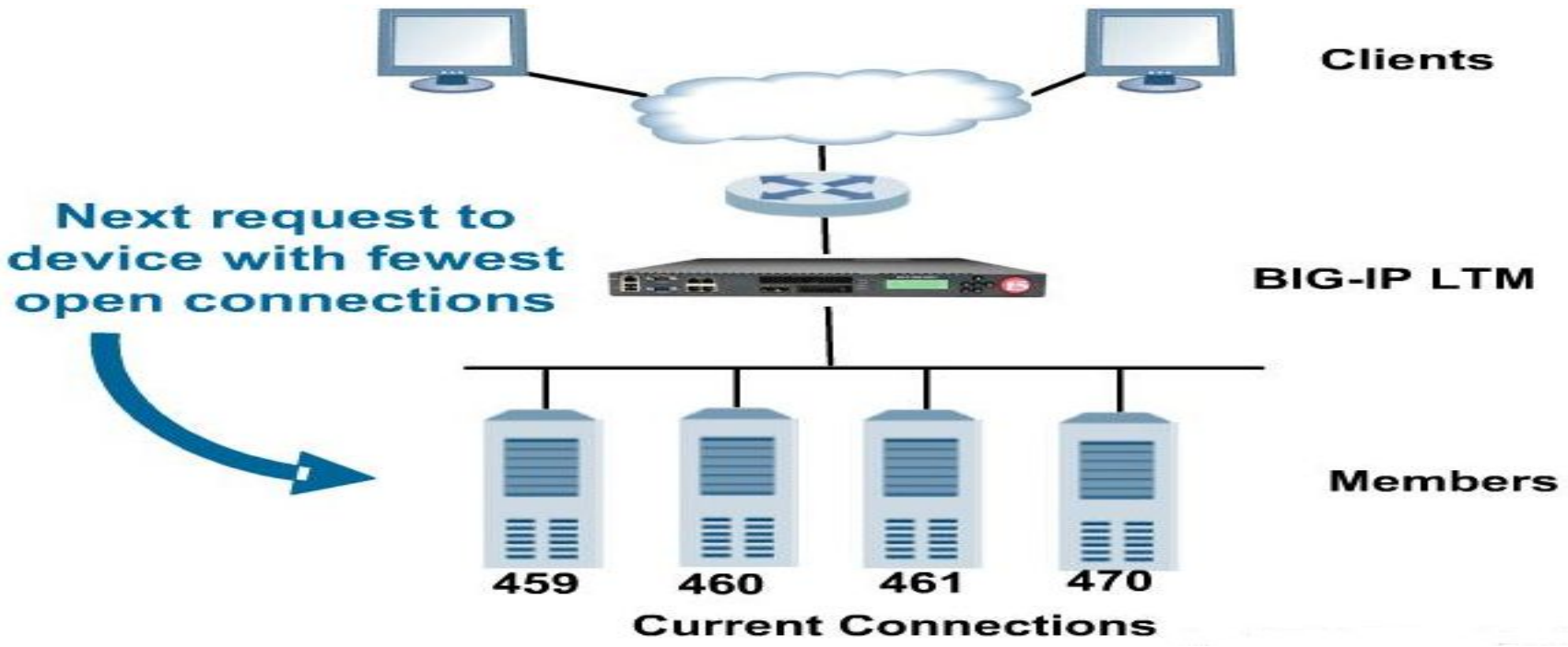
Ratio

-Ratio method is appropriate to use if some of the members are powerful than other.

-Since Ratio is static method, this means that server with highest ratio value will receive more request then others even if the performance of the server is slow.

Least Connections

- This method consider the current connections count to decide where to send next request



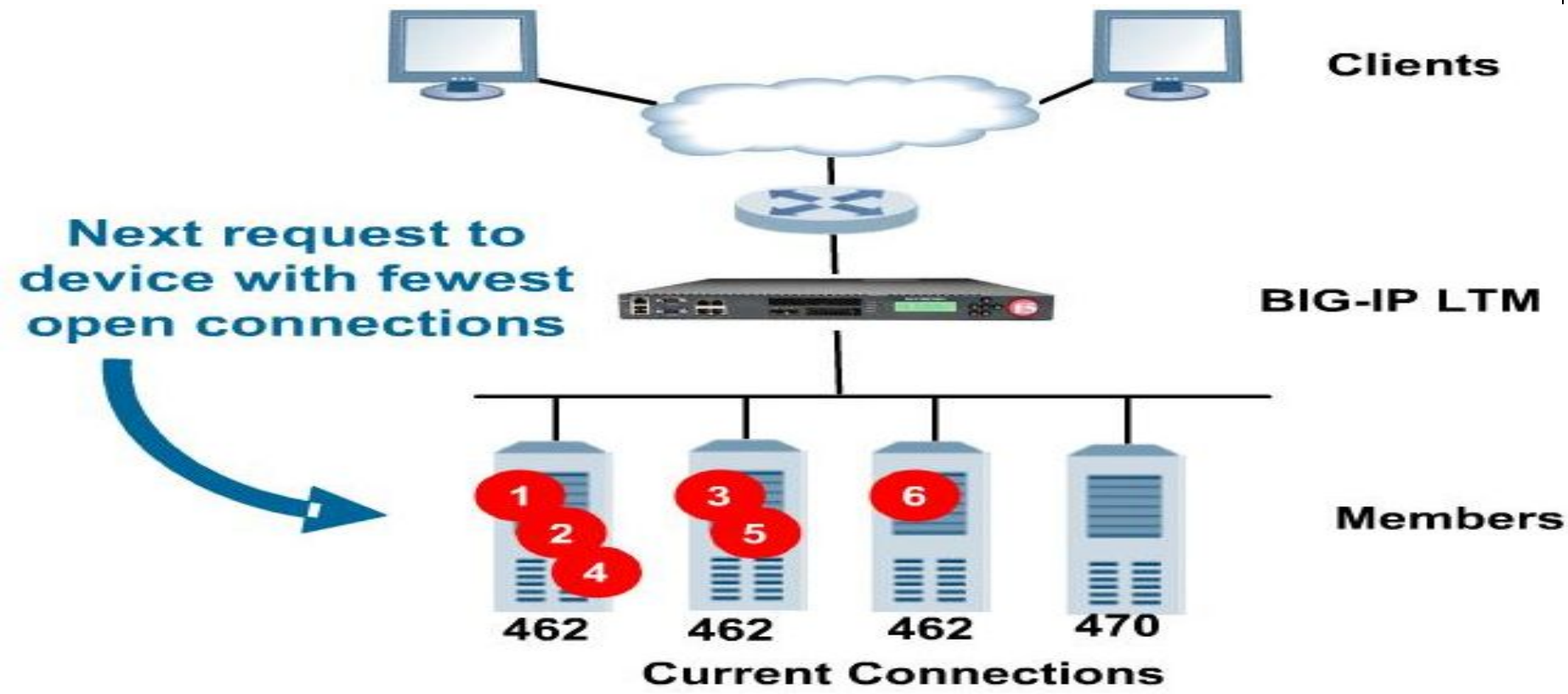
Dynamic Load Balancing

- Here F5 will take into consideration the load balancing mechanism. In static F5 would simply forward the packets.
- The various types of Load balancing methods are:

- Least Connection
- Observed
- Predictive
- Fastest

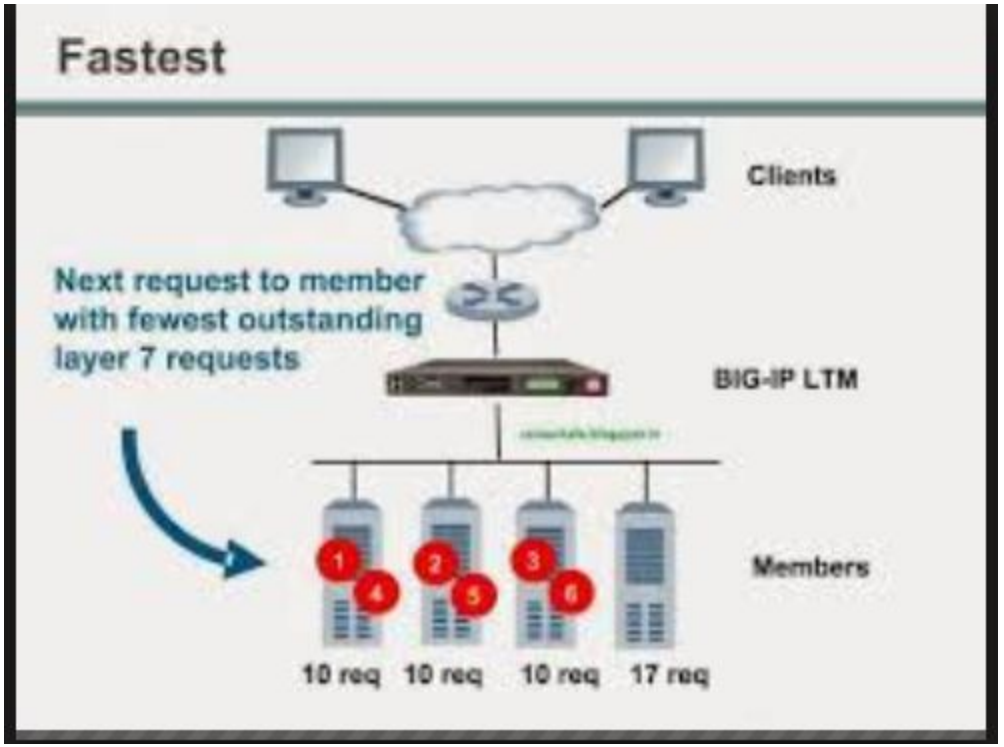
Least Connections

-After connections counts shown below, the big-IP round robin next requests between all three servers.



Fastest

-Fastest uses the outstanding layer 7 request to decide where to send the next request



Fastest

-Ping response form server doesn’t take into account how fast server will response at port 80.

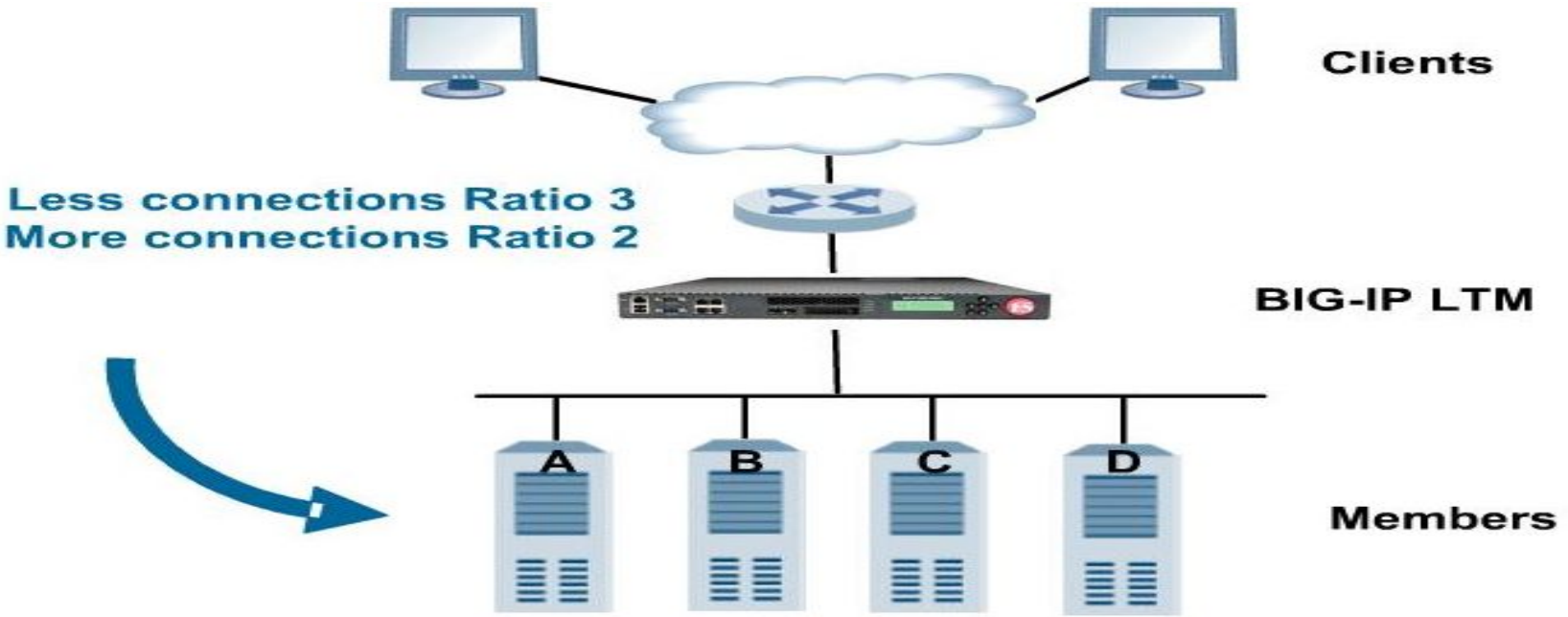
-SYN-ACK response form server at port 80 doesn’t take into account how fast backend database server will populate the content of web page

Observed

-It is basically Ratio load balancing but with Ratio assigned by Big-IP

-Servers with connections lower than average will given ratio of 3

-Servers with connections higher than average will given ratio of 2

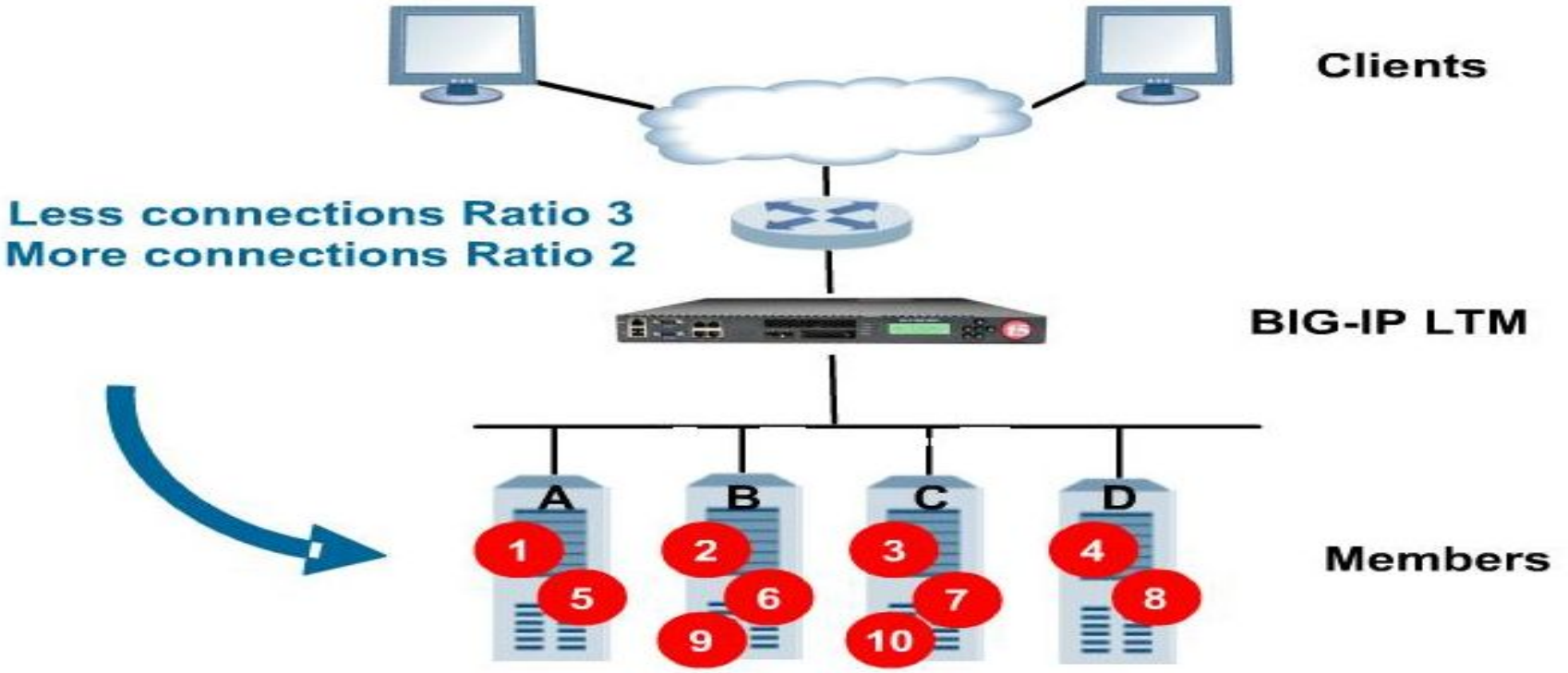


Observed

>Connections status

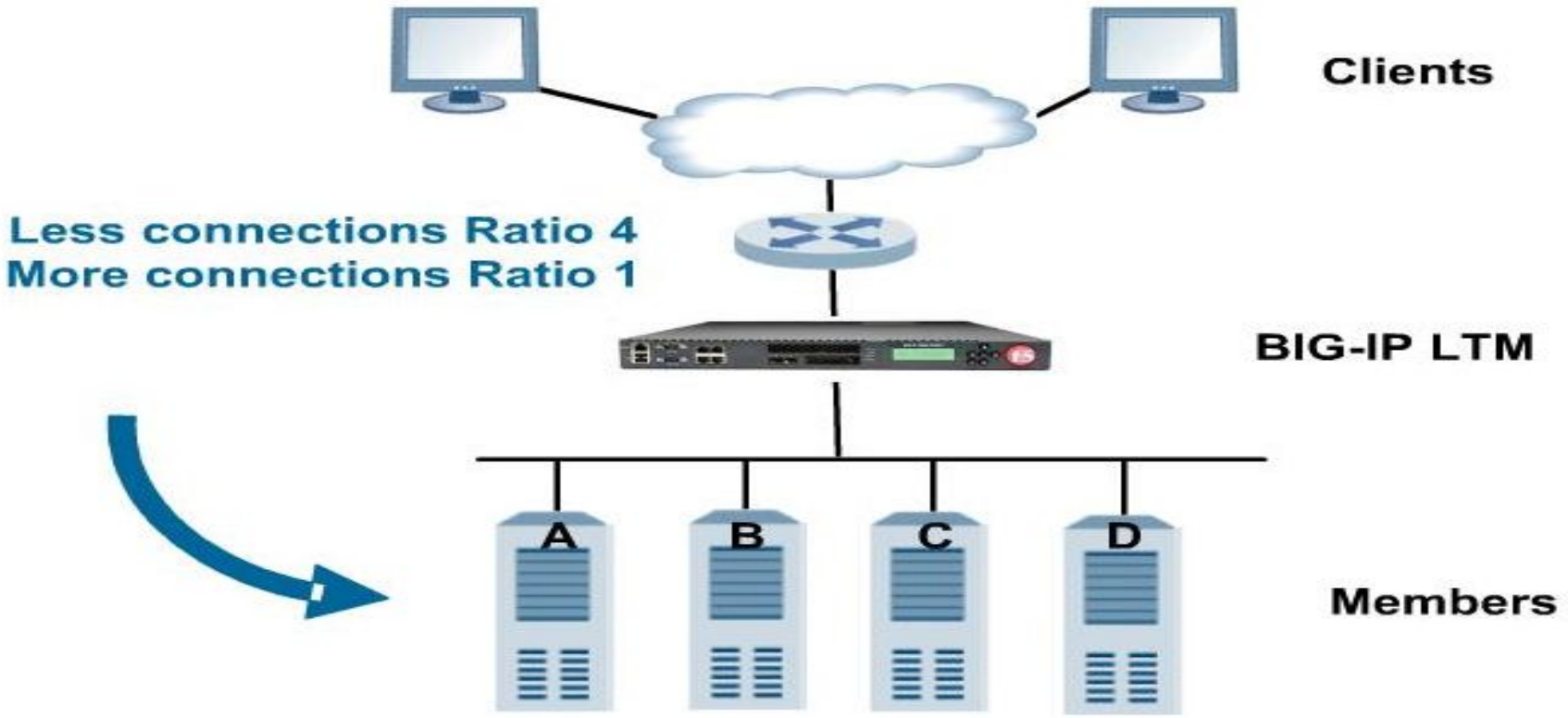
-server B & C with Ratio 3

-Servers A & D with Ration 2



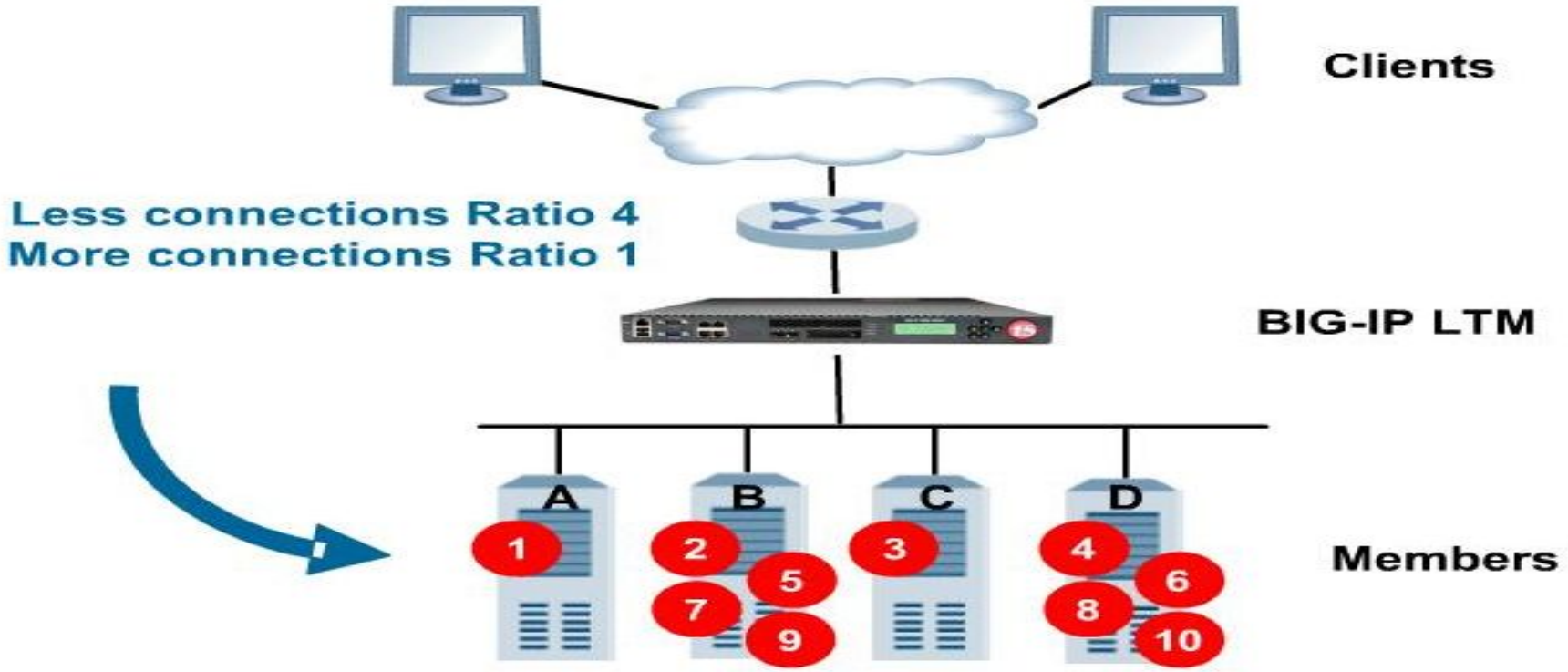
Predictive

-Predictive method is similar to Observed, but assigns more aggressive value



Predictive

>Connections status
 -server A & C with Ratio 1
 -Servers B & D with Ration 4



Pool Member vs. Node

- **Load Balancing by:**

>Node

-Total service for one IP Address

-Take all transactions for the IP address into account

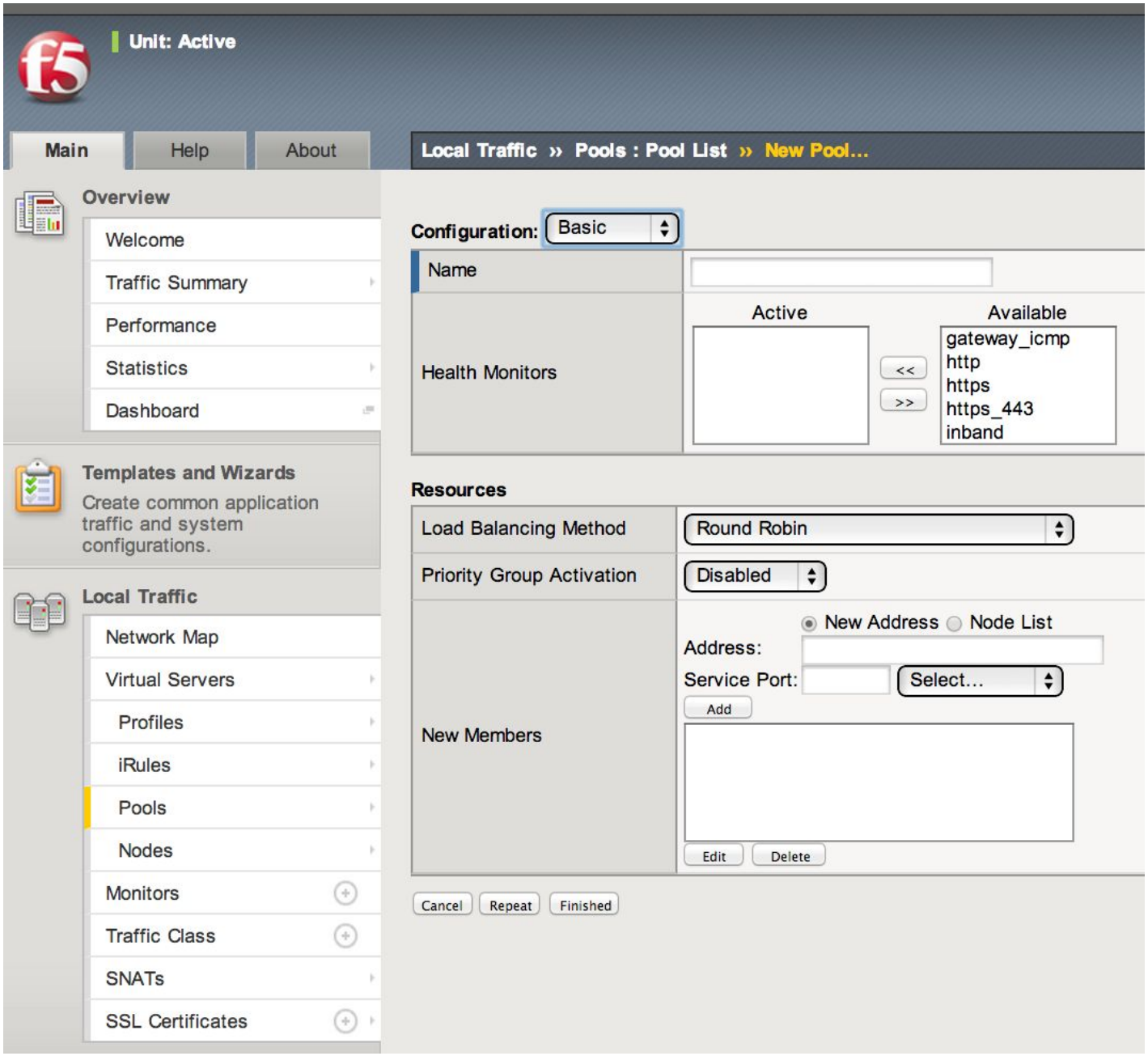
>Pool Member

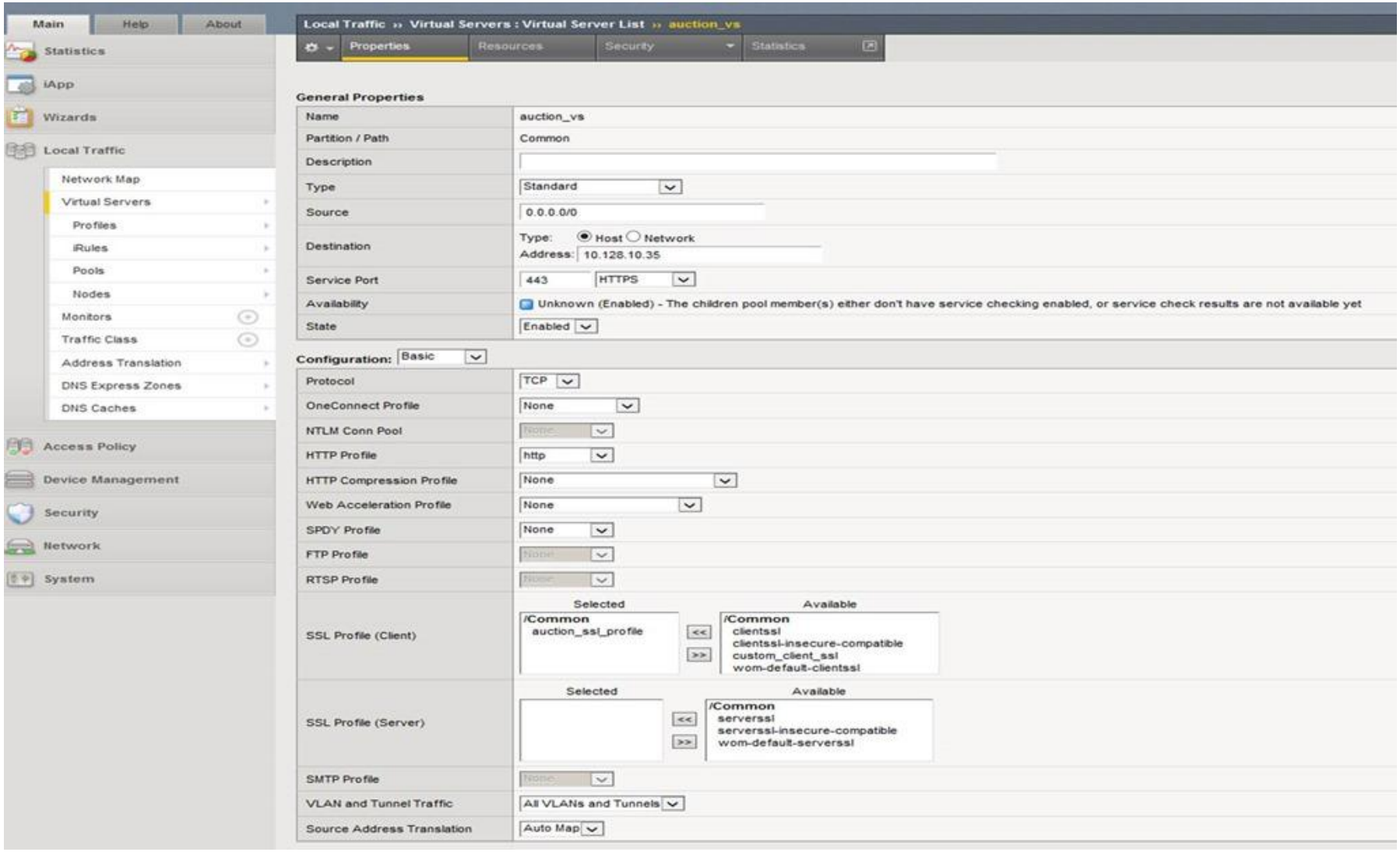
-IP Address & Service

-Take the decision based transactions happening on the service port.

Virtual Server configuration

- Create the node
- Create the pool member
- Assign Health Monitor
- Create virtual server


Unit: Active
Main
Help
About
Local Traffic » Pools : Pool List » New Pool...
Overview
Welcome
Traffic Summary
Performance
Statistics
Dashboard
Templates and Wizards
Create common application traffic and system configurations.
Local Traffic
Network Map
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
Traffic Class
SNATs
SSL Certificates
Configuration: Basic
Name
Active
Available
Health Monitors
<<
>>
gateway_icmp
http
https
https_443
inband
Resources
Load Balancing Method
Round Robin
Priority Group Activation
Disabled
New Address
Node List
Address:
Service Port:
Select...
Add
New Members
Edit
Delete
Cancel
Repeat
Finished


Main
Help
About
Statistics
iApp
Wizards
Local Traffic
Network Map
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
Traffic Class
Address Translation
DNS Express Zones
DNS Caches
Access Policy
Device Management
Security
Network
System
Local Traffic ›› Virtual Servers : Virtual Server List ›› auction_vs
Properties
Resources
Security
Statistics
General Properties
Name
auction_vs
Partition / Path
Common
Description
Type
Standard
Source
0.0.0.0/0
Destination
Type: Host Network
Address: 10.128.10.35
Service Port
443
HTTPS
Availability
Unknown (Enabled) - The children pool member(s) either don't have service checking enabled, or service check results are not available yet
State
Enabled
Configuration: Basic
Protocol
TCP
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Profile
http
HTTP Compression Profile
None
Web Acceleration Profile
None
SPDY Profile
None
FTP Profile
None
RTSP Profile
None
SSL Profile (Client)
Selected
/Common
auction_ssl_profile
Available
/Common
clientssl
clientssl-insecure-compatible
custom_client_ssl
wom-default-clientssl
SSL Profile (Server)
Selected
Available
/Common
serverssl
serverssl-insecure-compatible
wom-default-serverssl
SMTP Profile
None
VLAN and Tunnel Traffic
All VLANs and Tunnels
Source Address Translation
Auto Map

Priority Group Activation

-Use to designate preferred & backup sets of pool members with in a pool

-Once priority group activated

-The available member with highest priority will consider first

Priority Group Activation

-If the number of member falls below the priority group activation set,

-The next highest priority member also start serving the requests.

Fallback Host

-Fallback host feature is designed for HTTP protocol only.

-It comes into play if all the members in a pool are unavailable

MODULE 5

Monitor

- ***Monitor Functionality***
- ***Monitor Types***
- ***Configuring Monitor***
- ***Assigning Monitor***
- ***Status***

Intro to monitor

- Big-IP system can monitor the health of nodes & member
- Monitor is the test that Big-IP performed

  -simple test

  -Highly interactive test

- The result of these test will define the status of respective node or member is available
- Big-IP perform continues monitoring irrespective of the status of node or member

Step to set-up a monitor

Step 1: Create

Step 2: Name & Type

-name the new monitor select the type from system templates

Step 3: Customize

Step 4: Assign

- to pool/node/pool member

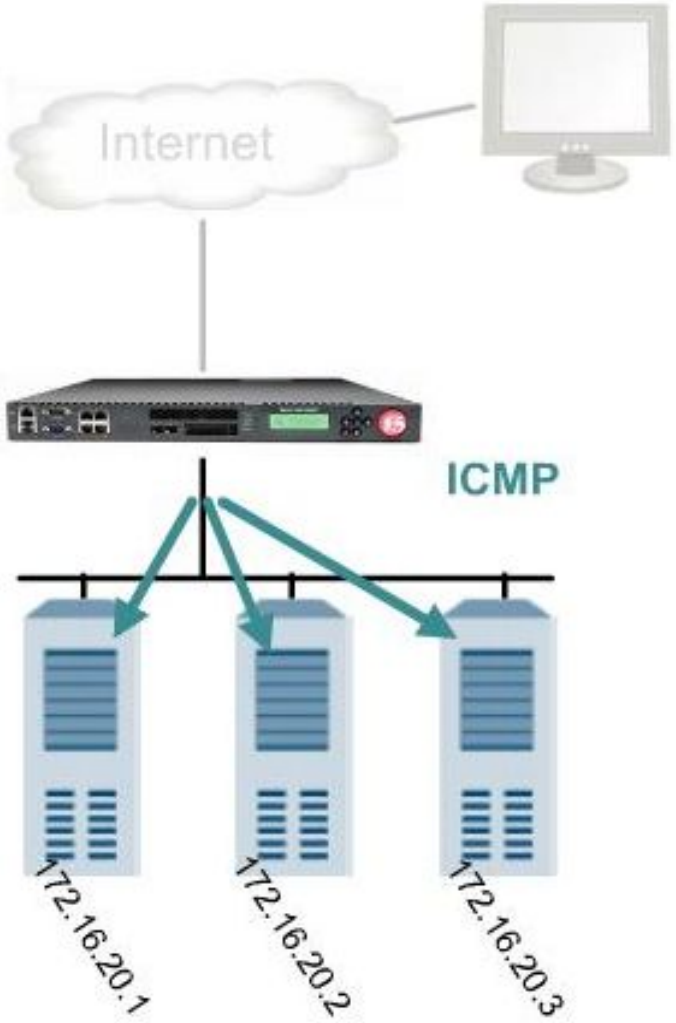
Step 5: Status

Types of monitoring

- Address Check
  -IP address –node
- Service Check
  -IP:port
- Content Check
  -IP:port & check data returned
- Interactive Check
  -Interactive with servers
  -Multiple commands and multiple response

Address Check

- Packets sent to IP Address
- If no response, Node Down
  - Members Down
  - No Connections to Members
- Example: ICMP

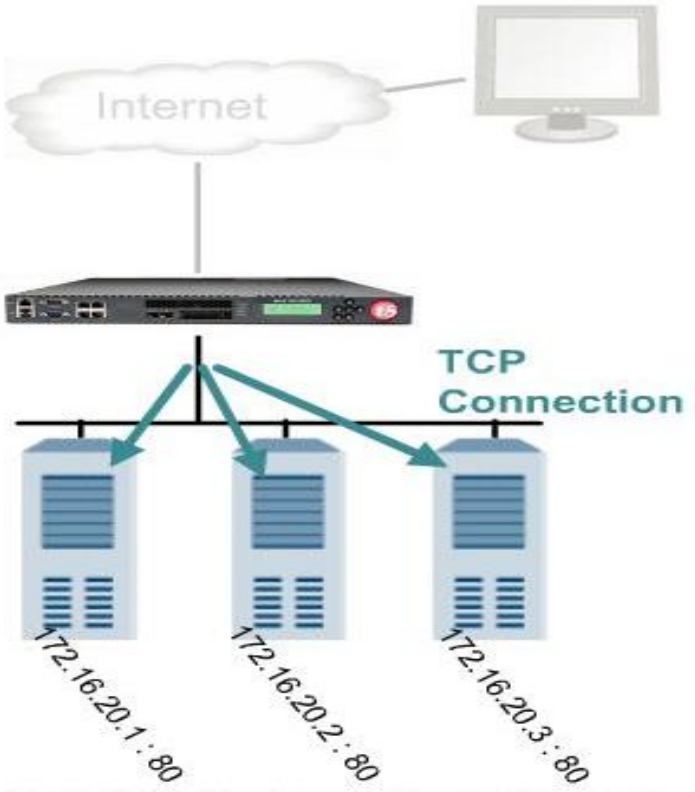


Service Check

-Service checks only test whether server is listening to respective port.

-Doesn’t provide any insight into quality of the content that might return

- TCP connection opened and closed
- If connection fails, Member Down
  - No Connections to Member
- Example: TCP



Content Check

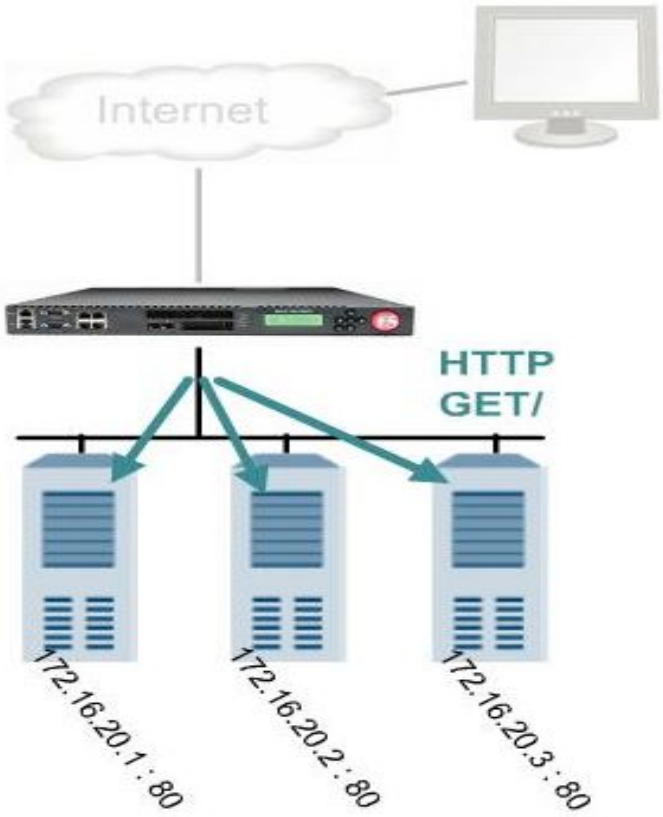
-Content check go beyond testing whether a node is responding/listening

-It also test if it is responding with correct content

- TCP connection opened
- Command Sent
- Response Examined
- Connection Closed

- If connection or response fails, Member Down
  - No Connections to Member

- Example: HTTP

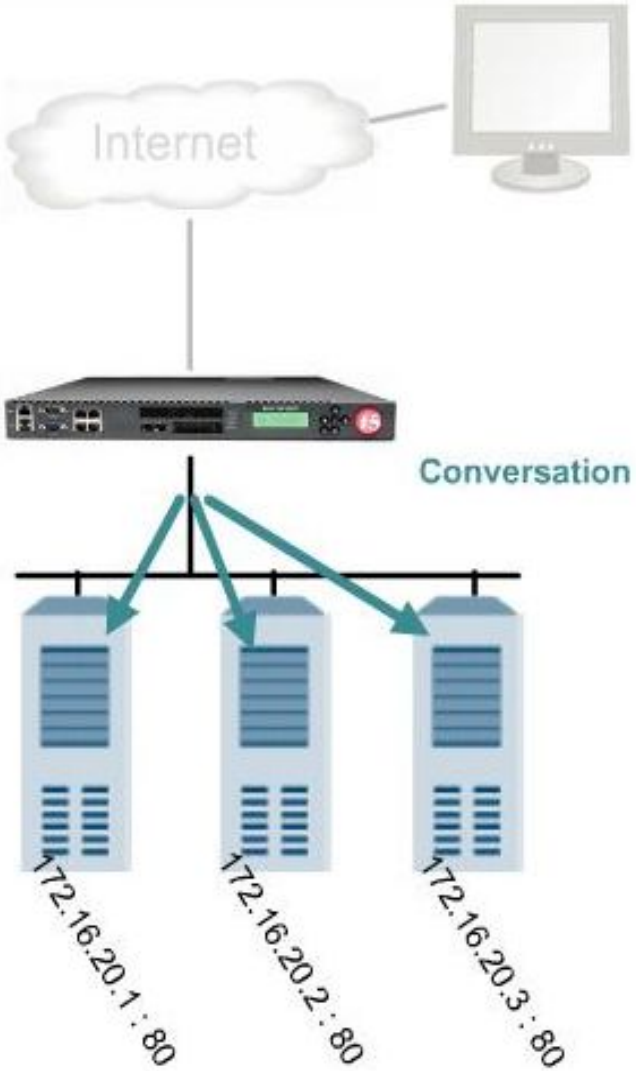


Interactive Check

- TCP connection(s) opened
- Command(s) Sent
- Response(s) Examined
- Connection(s) Closed

- If the Condition fails, Member Down
  - No Connections to Member

- Example: FTP

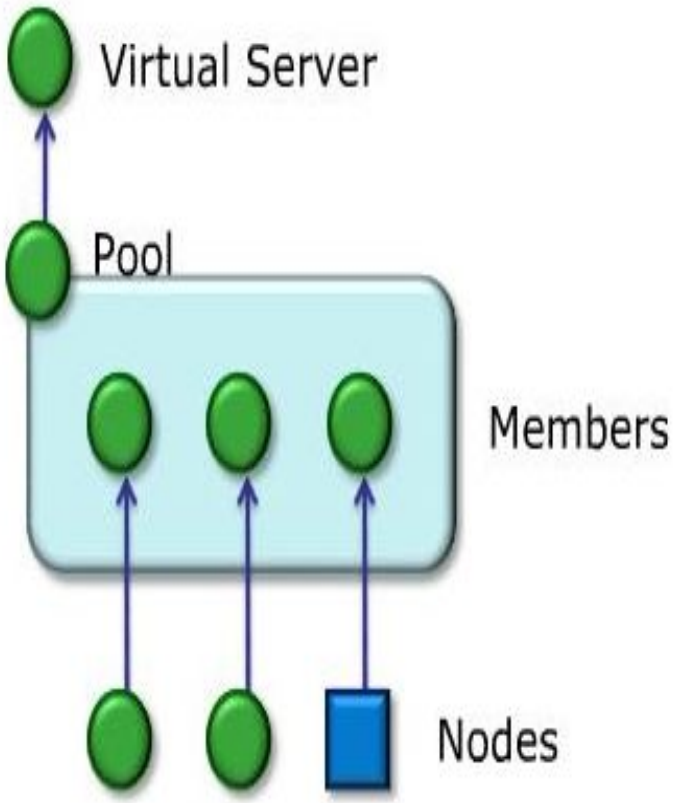


Status Icon

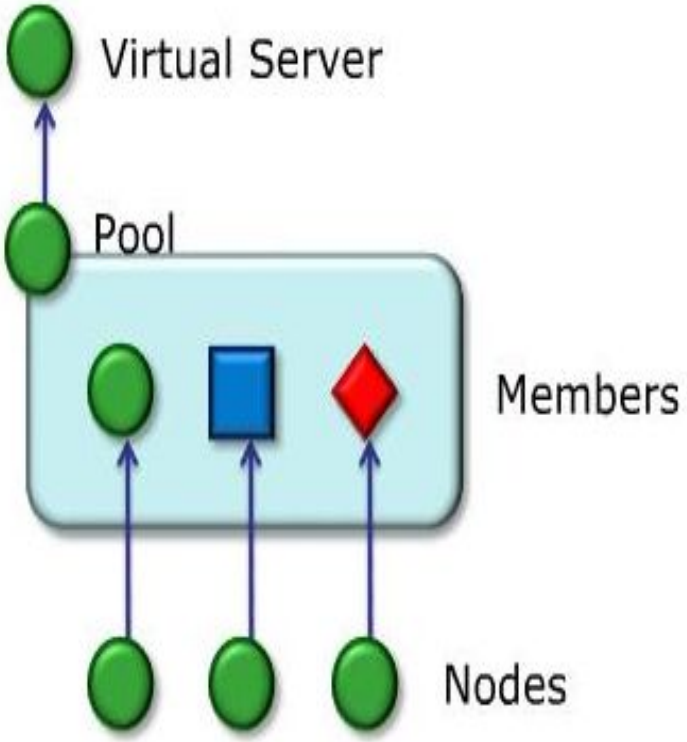
- Below are the status Icons

Status: Available

- Example-1

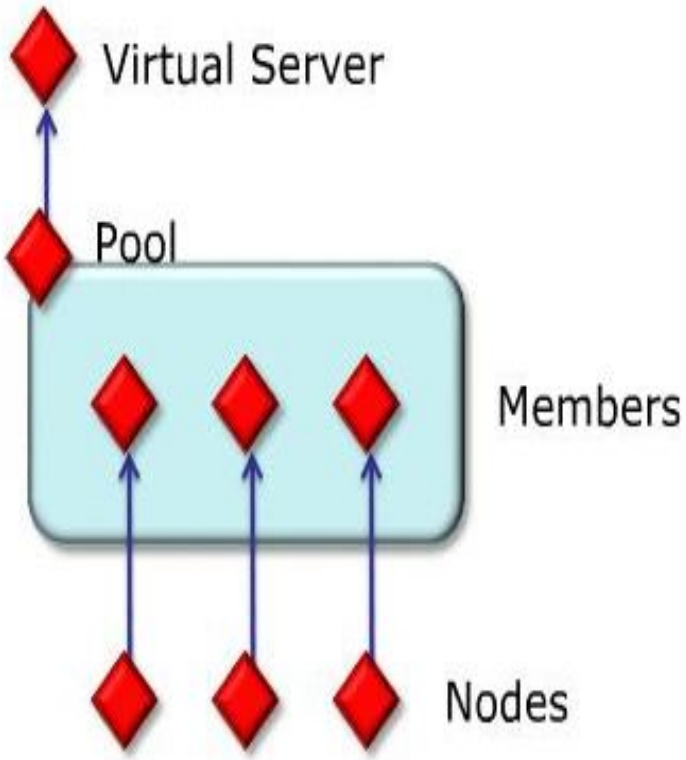


- Example-2

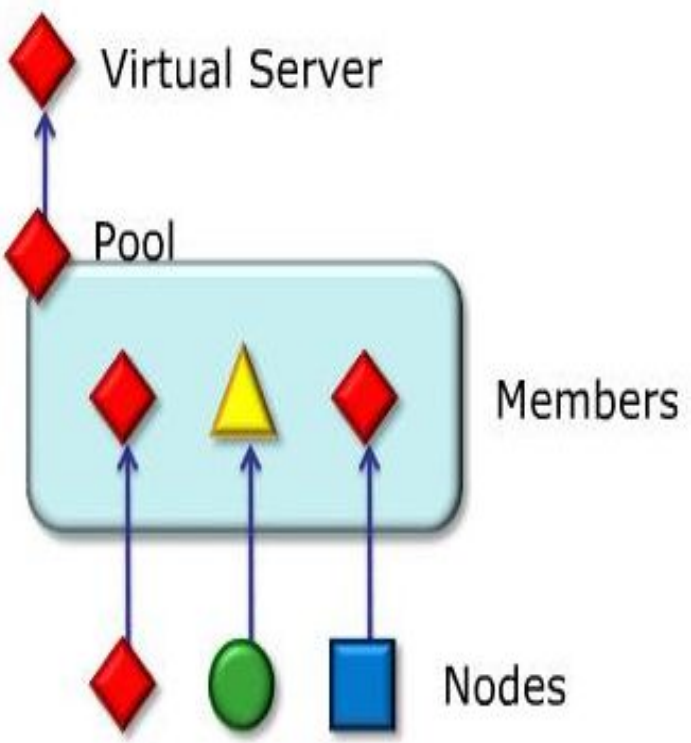


Status: Offline

- Example-1

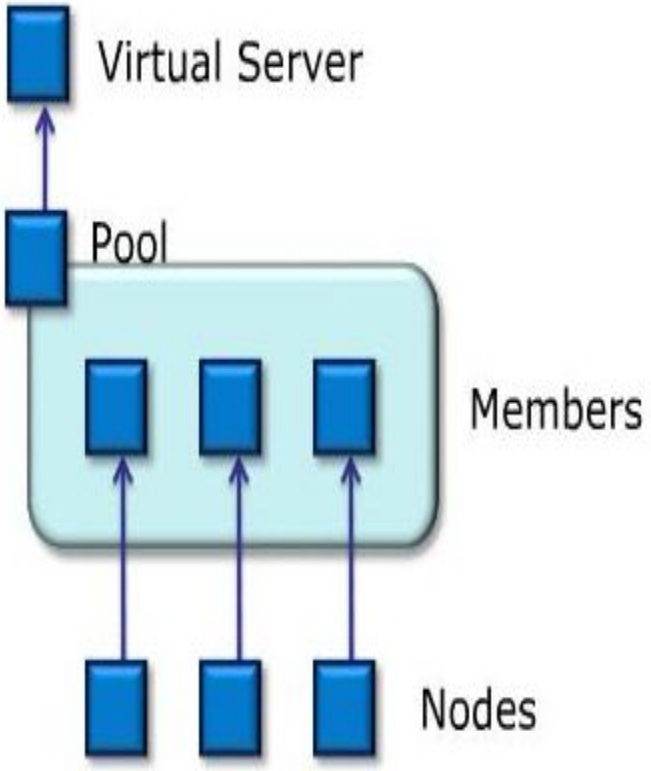


- Example-2

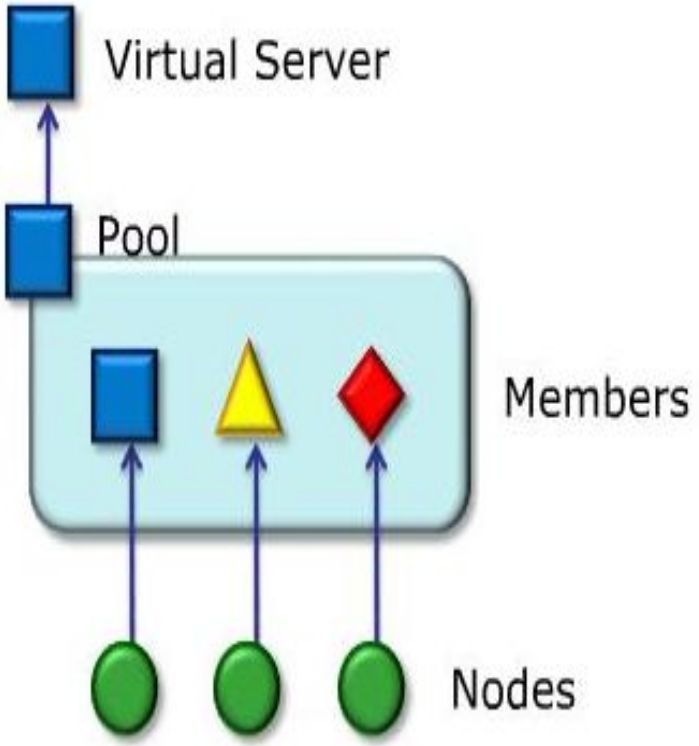


Status: Unknown

- Example-1

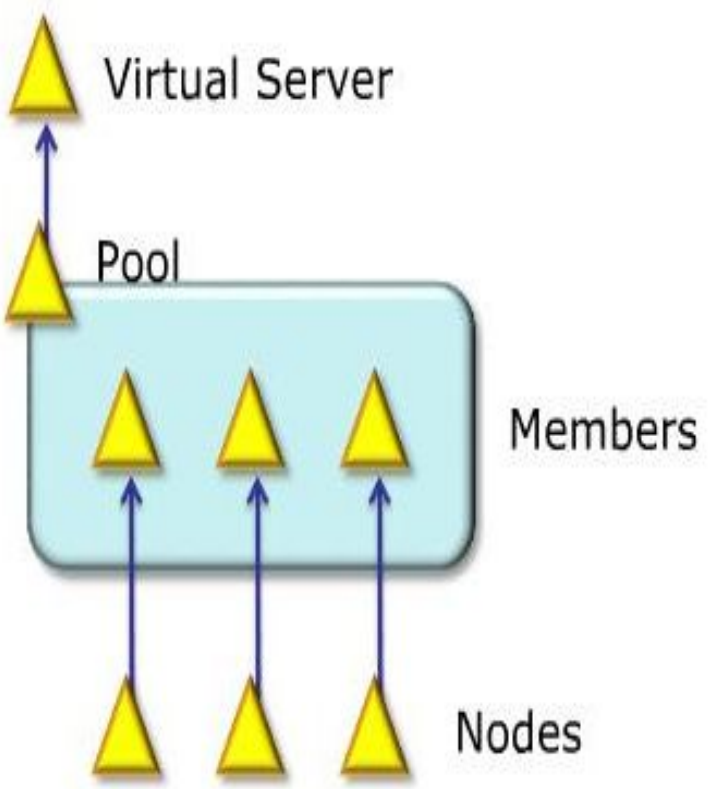


- Example-2

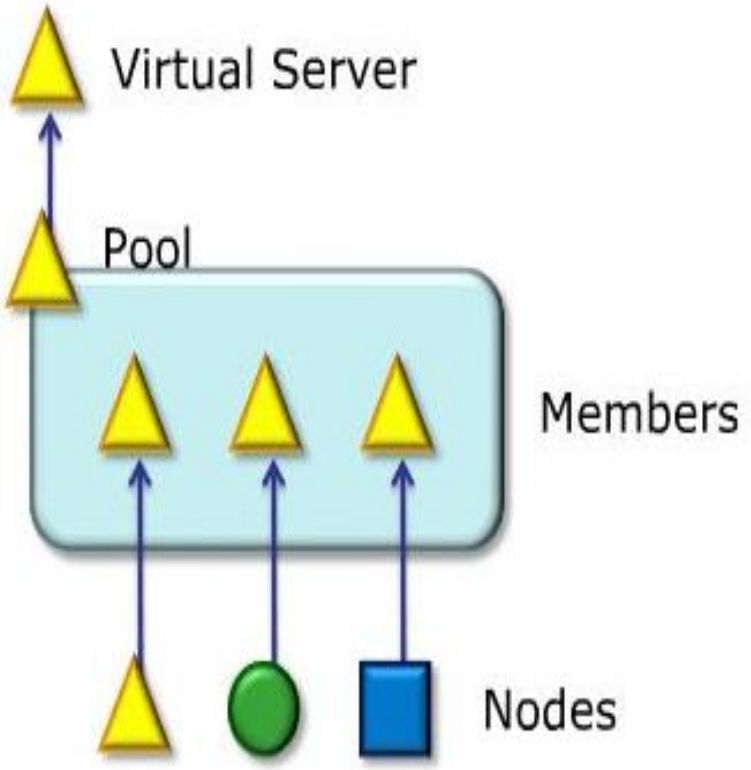


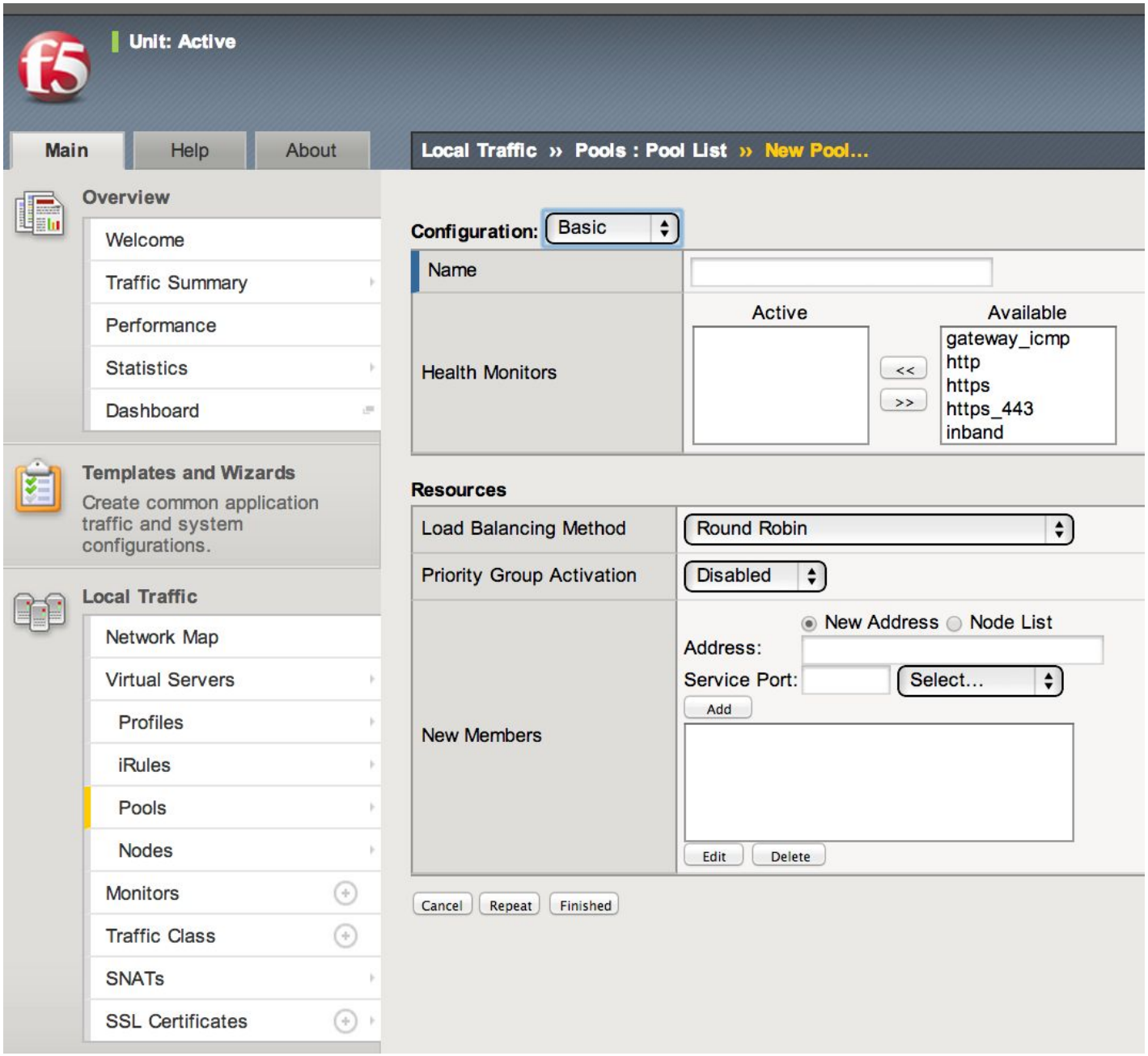
Status: Unavailable

- Example -1



- Example -2




Unit: Active
Main
Help
About
Local Traffic » Pools : Pool List » New Pool...
Overview
Welcome
Traffic Summary
Performance
Statistics
Dashboard
Templates and Wizards
Create common application traffic and system configurations.
Local Traffic
Network Map
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
Traffic Class
SNATs
SSL Certificates
Configuration: Basic
Name
Active
Available
Health Monitors
<<
>>
gateway_icmp
http
https
https_443
inband
Resources
Load Balancing Method
Round Robin
Priority Group Activation
Disabled
New Address
Node List
Address:
Service Port:
Select...
Add
New Members
Edit
Delete
Cancel
Repeat
Finished

MODULE 6

Profile

- ***Profile Concept***
- ***Profile Configuration***

Profile Concept

- Contain settings that instruct how to pass the traffic through virtual server
- Why any one want to change default traffic processing behavior of virtual server ?
- Are profile overrides the load balancing property ?
- How does profile help to improve the performance of actual servers ?

Profiles are a configuration tool that you can use to affect the behavior of certain types of network traffic. More specifically, a ***profile*** is an object that contains settings with values, for controlling the behavior of a particular type of network traffic, such as HTTP requests and responses.

- You can use the default profiles, which means that you do not need to actively configure any profile settings. The BIG-IP system uses them to automatically direct the corresponding traffic types according to the values specified in the those profiles.

- You can create a custom profile, using the default profile as the parent profileA ***custom profile*** is a profile derived from a default profile and contains values that you specify.

- You can create a custom profile to use as a parent profile for other custom profiles.

- After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Types of profile

- Services Profiles:

-HTTP, FTP, RSTP, SIP, iSession

- Persistence Profiles

-cookie, dest_addr, source_addr, hash….

- Protocol Profiles

-tcp, udp, fastL4…

- SSl Profiles

-client, server

- Authentications Profiles

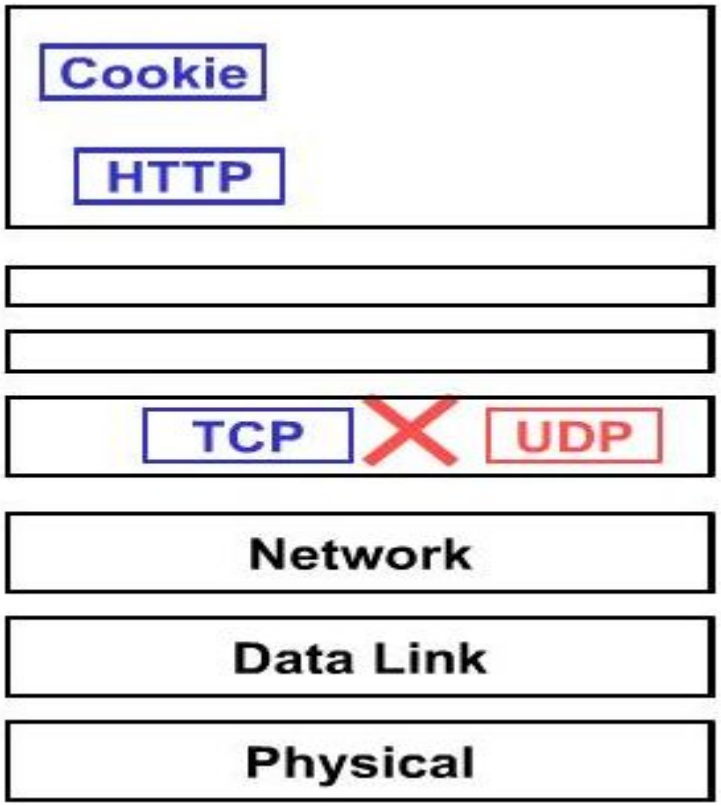
-RADIUS servers, CRLDP servers...

- Other Profiles

-OneConnect, NTLM, stream

Profile Dependencies

-Some of the profiles are dependent on others
-Some can’t be combine in one VS



Profile Configuration Concepts

- Default Profiles – Tamplates

  -Stored in /config/profile_base.conf

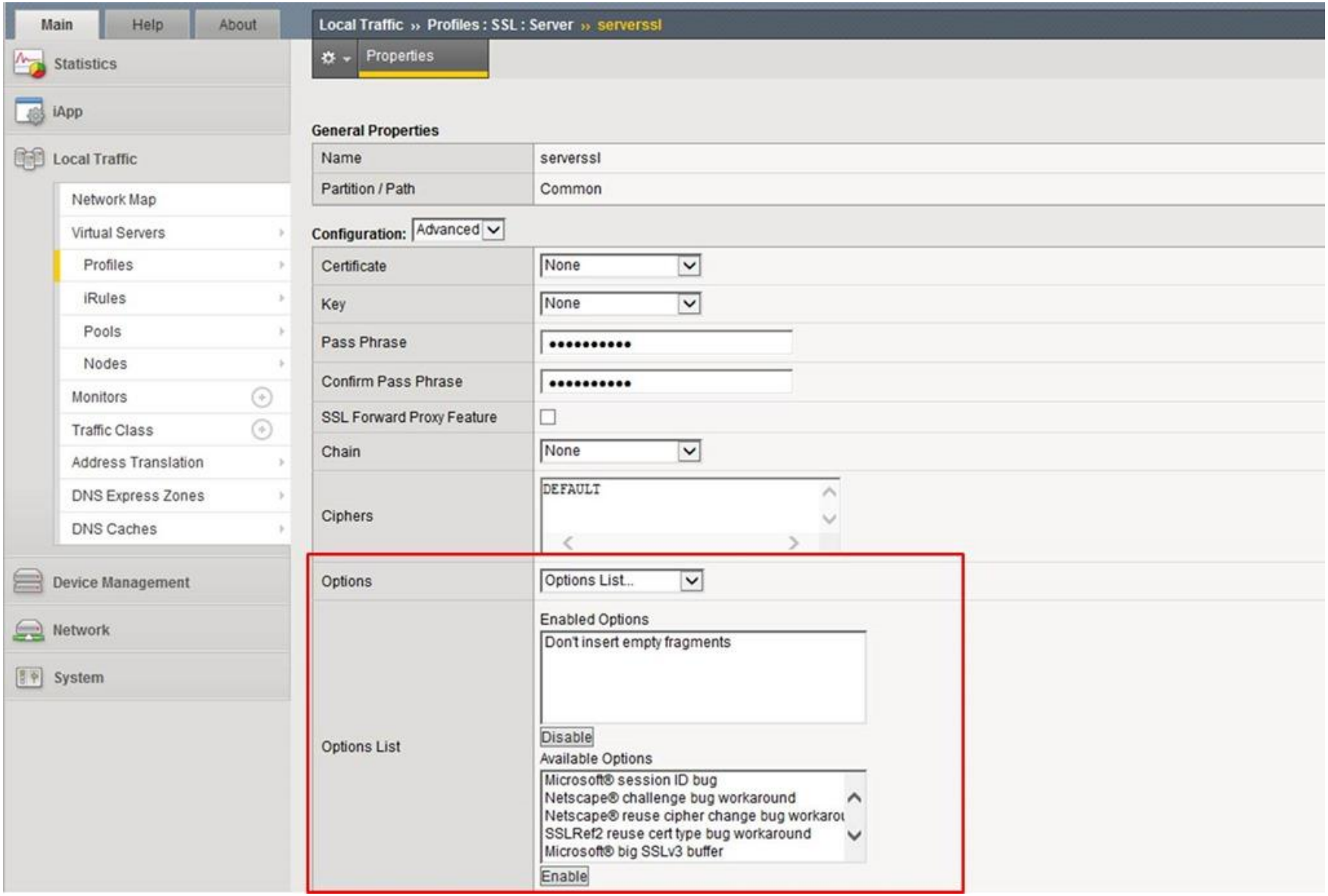
  -Can’t be deleted

- Custom Profiles

  -Stored in /config/bigip.conf

  -Created from default profile

  -Dynamic child & parent relationship


Main
Help
About
Statistics
iApp
Local Traffic
Network Map
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
Traffic Class
Address Translation
DNS Express Zones
DNS Caches
Device Management
Network
System
Local Traffic » Profiles : SSL : Server » serverssl
Properties
General Properties
Name
serverssl
Partition / Path
Common
Configuration: Advanced
Certificate
None
Key
None
Pass Phrase
Confirm Pass Phrase
SSL Forward Proxy Feature
Chain
None
Ciphers
DEFAULT
Options
Options List...
Options List
Enabled Options
Don't insert empty fragments
Disable
Available Options
Microsoft® session ID bug
Netscape® challenge bug workaround
Netscape® reuse cipher change bug workarou
SSLRef2 reuse cert type bug workaround
Microsoft® big SSLv3 buffer
Enable

MODULE 7

Persistence

- ***Persistence profile***
- ***Source Address Persistence***
- ***Cookie Persistence***

Concept

- What is the need of Persistence ?
- Persistence profile is required to achieve to change the load balancing behavior of virtual server
- Upon the initial connection:

-Big-IP store session data in persistence record

- Persistence Record store

-client characteristics

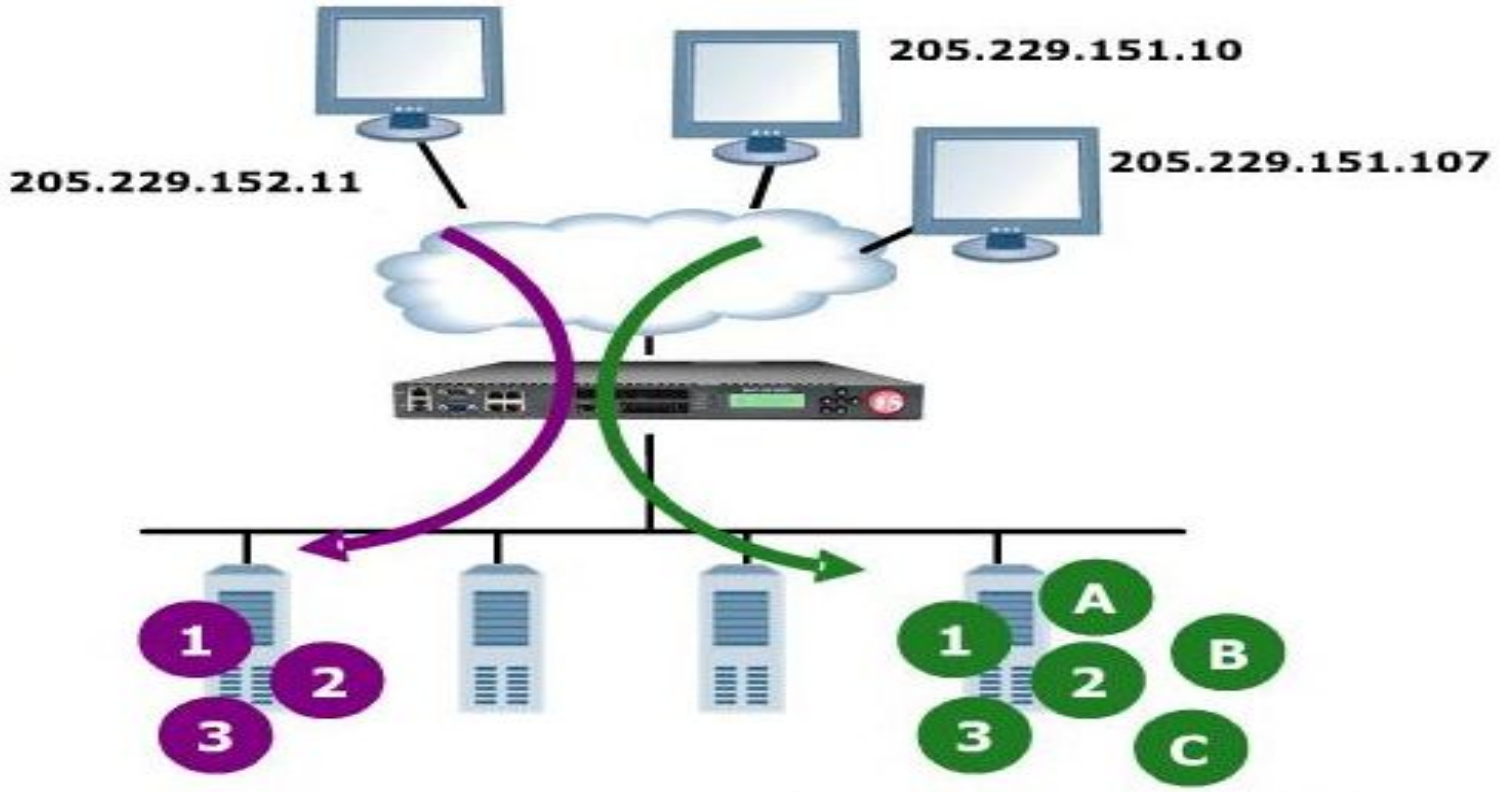
-Pool member information which is serving request

- Big-IP use persistence record to serve the next traffic

Source Address Persistence

-Support both TCP & UDP protocol

-By Default Big-IP create persistence for host



Cookie Persistence

- Why cookie Persistence ?
- Modes:

>Insert Mode

-LTM insert special cookie in HTTP response

-Pool name & Pool Member (encoded)

>Rewrite Mode

-Web server Creates a “blank” cookie

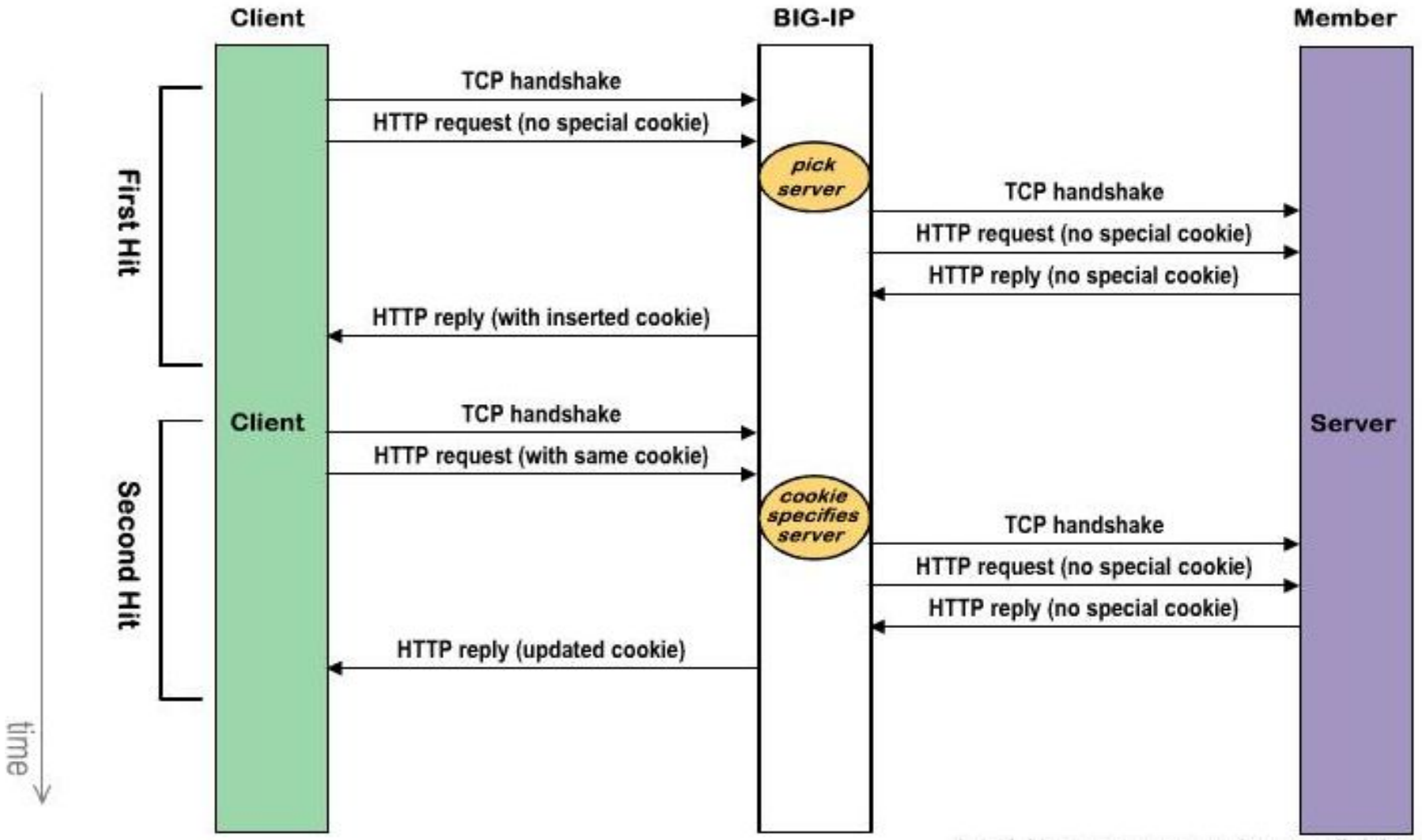
-LTM Rewrites to make Special Cookie

>Passive Mode

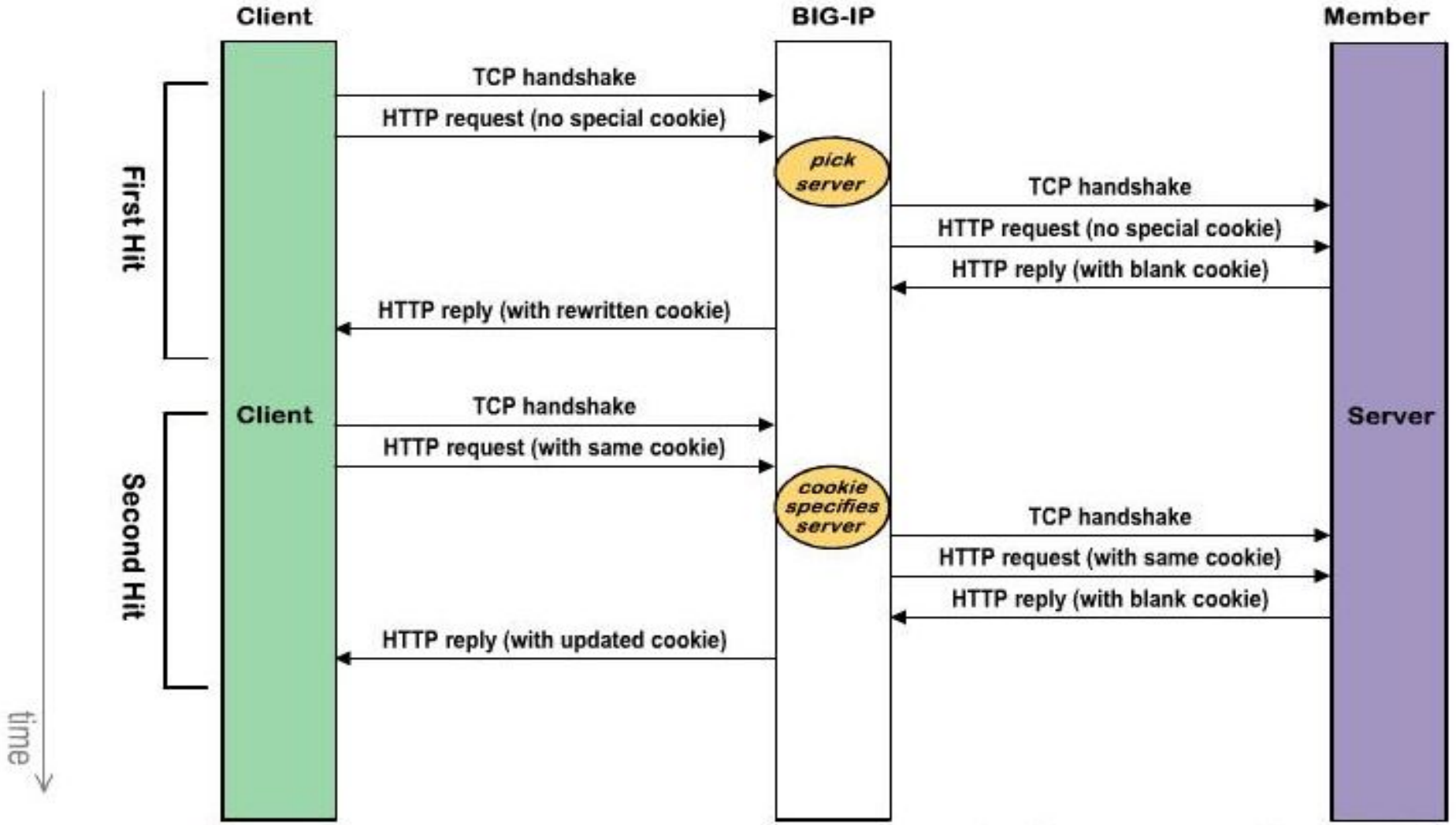
-Web server Creates Special Cookie

-LTM Passively lets it through

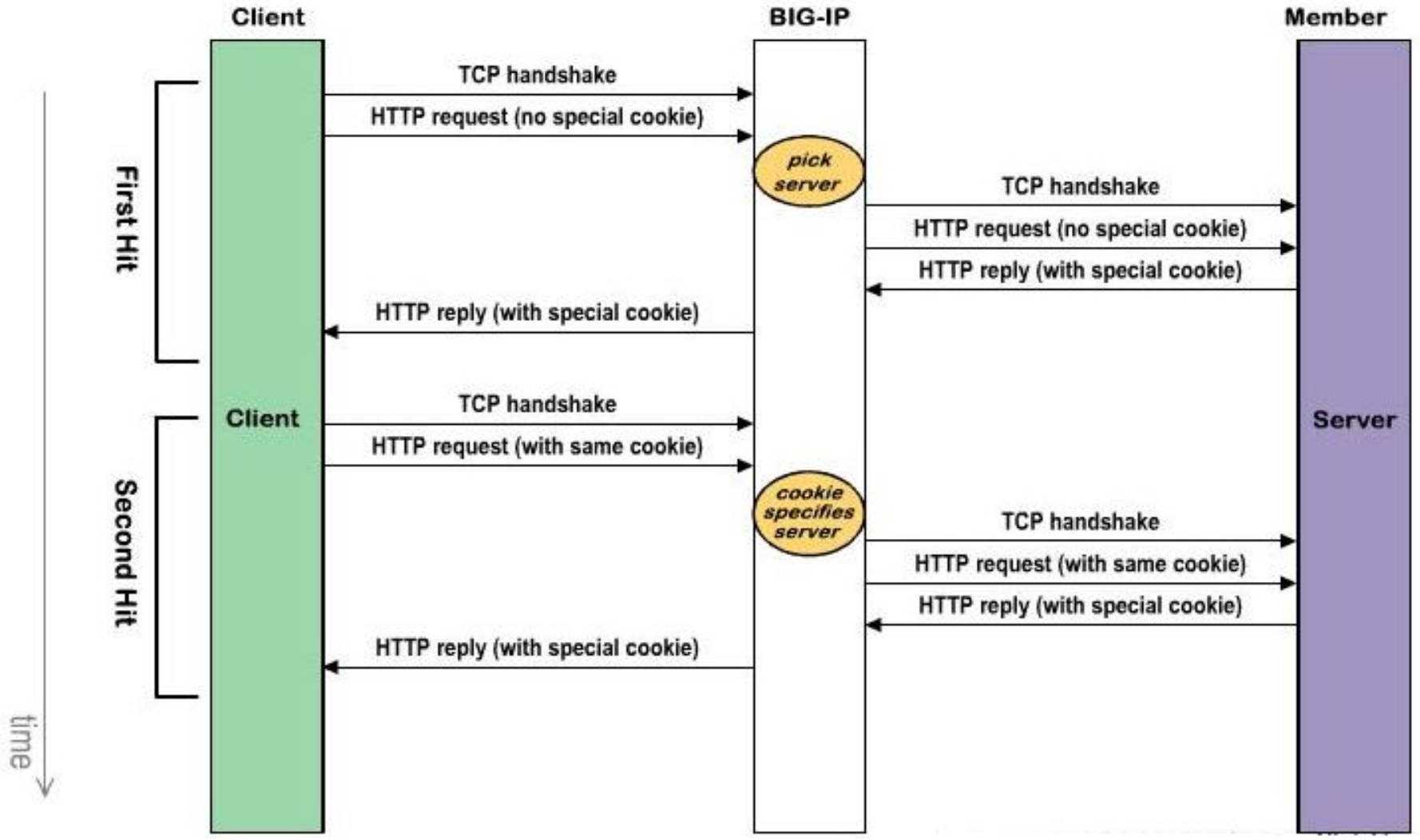
Cookie Insert Mode

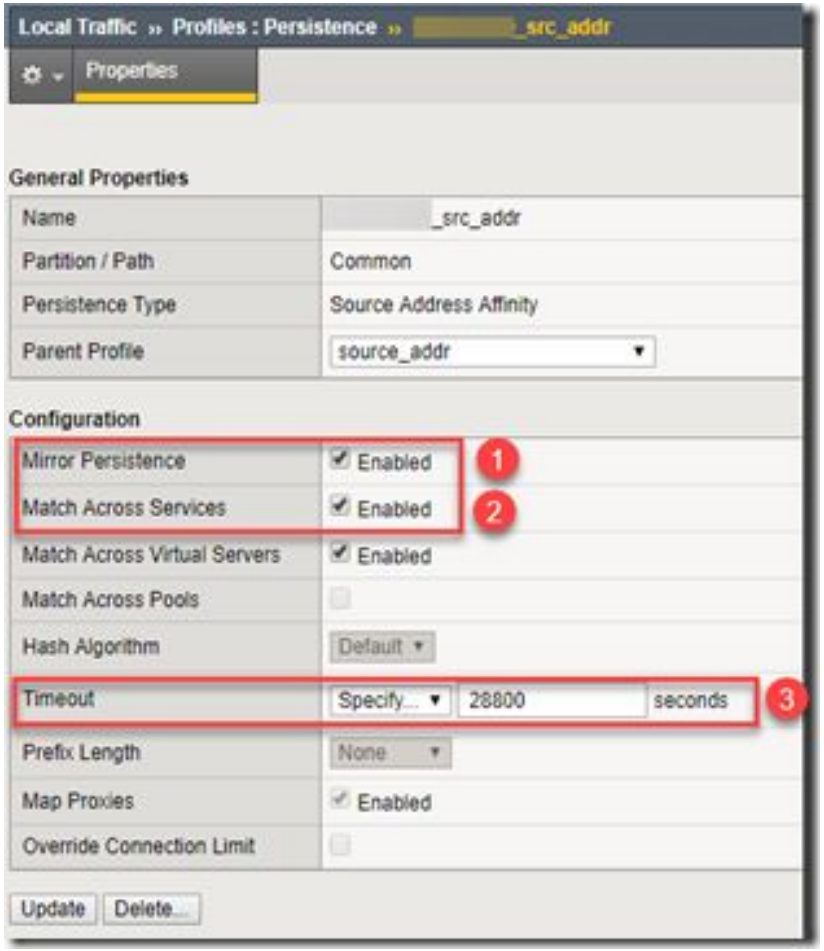


Cookie Rewrite Mode

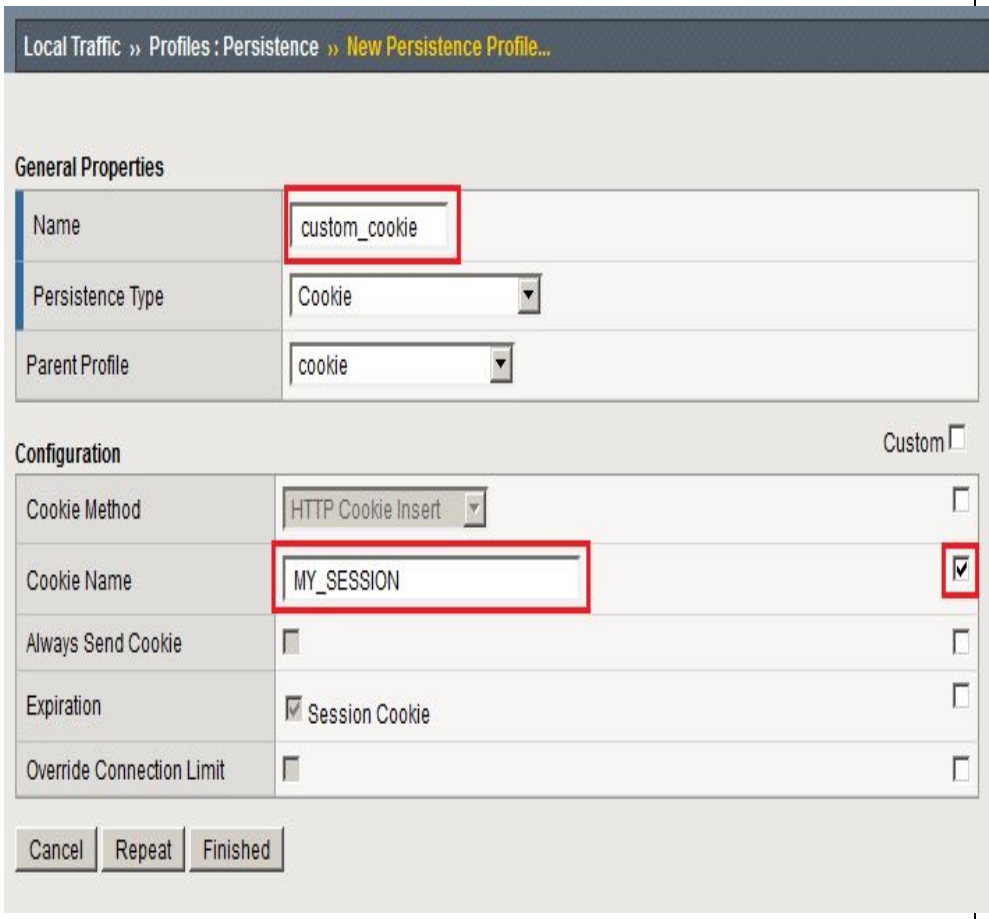


Cookie Passive Mode





IP
Based



Cookie
Based

MODULE 8

Processing SSL Traffic

- ☐ ***Exploring SSL on Big-IP***
- ☐ ***Configuring Big-IP for SSL***

Advantage of SSL Termination

- Allow iRules processing and cookie persistence
- Offload SSL traffic from web server
- SSL key exchange and bulk encryption dane by hardware
- Centralize certificate management

What is an SSL Certificate?

The certificate is nothing more than a document containing the public key the client will use to compute key material and information about expiration, common and distinguished names, contact information, etc. A certificate can be modified until it is signed. This can be done to itself, which would be a self-signed certificate (all root certificates are self-signed) or a certificate can be signed by a certificate authority (CA).

Figure 1. SSL Certificate

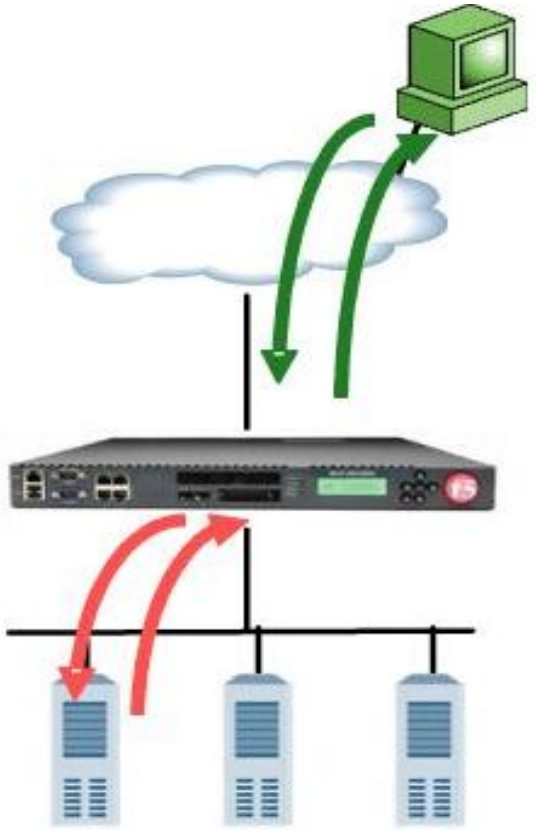
Traffic Flow: Client SSL

Client sends encrypted packet, BIG-IP receives it and decrypts it.

BIG-IP processes packet, sends to Pool member using load balancing.

Pool member processes unencrypted request, sends unencrypted response to BIG-IP

BIG-IP encrypts response and sends to client.



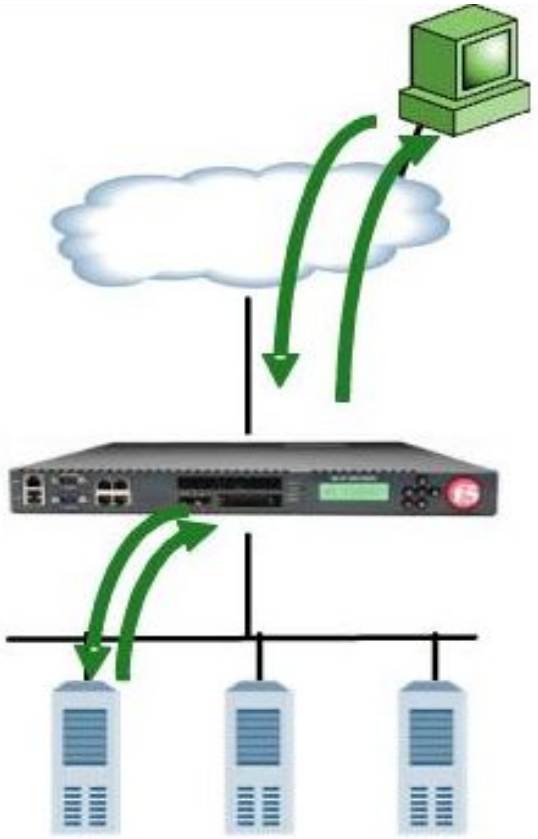
Traffic Flow: Server SSL

Client initiates SSL connection and BIG-IP decrypts it.

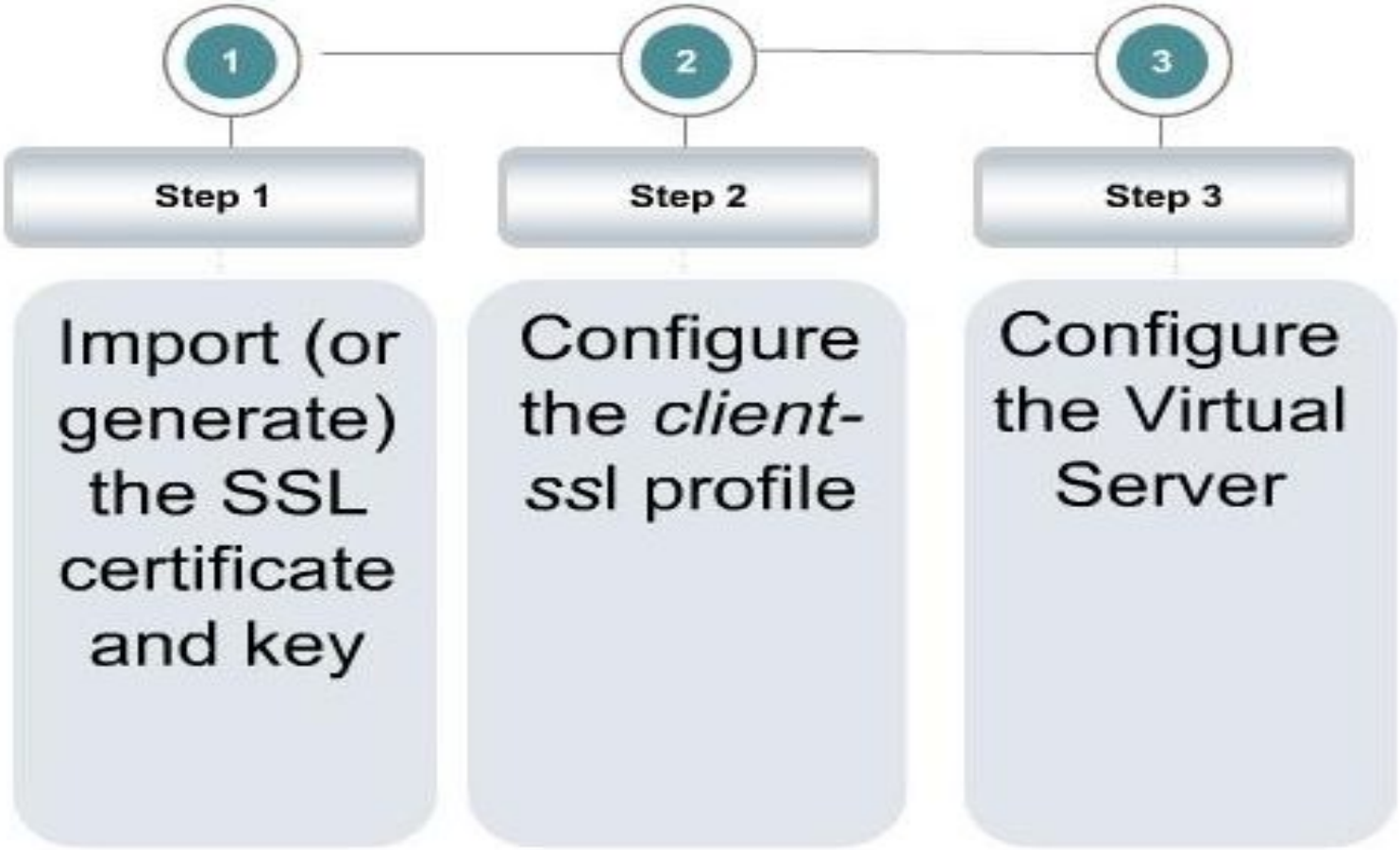
BIG-IP re-encrypts traffic with different SSL cert and key, and sends it to Pool member.

Pool member decrypts packet, processes it, re-encrypts response, and sends it to BIG-IP

BIG-IP decrypts response, processes it, re-encrypts it, and sends back to client.



Enabling Client SSL Profile



MODULE 9

Nat & SNAT

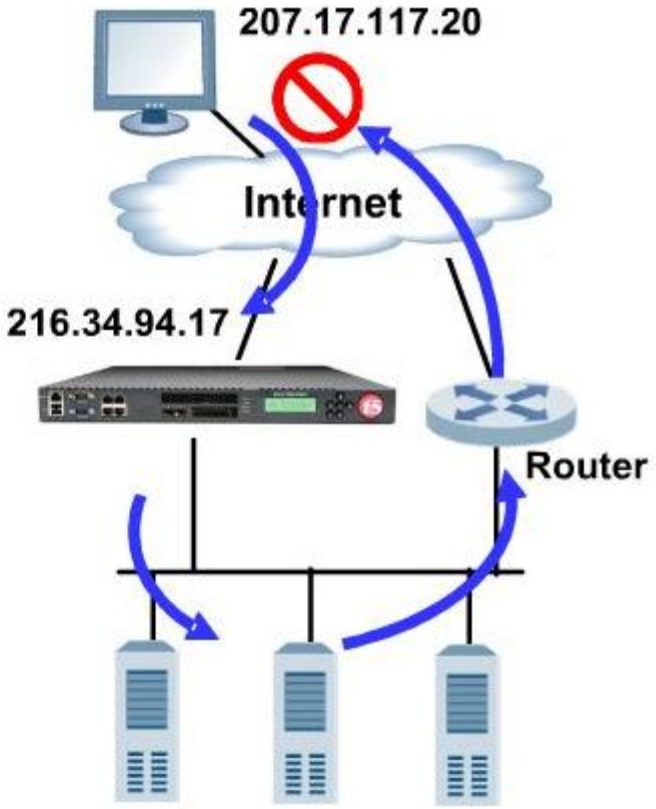
- ***NAT Concepts and Configuration***
- ***SNAT Concepts and Configuration***

Asymetric Routing Problem

Response packet must return through BIG-IP.

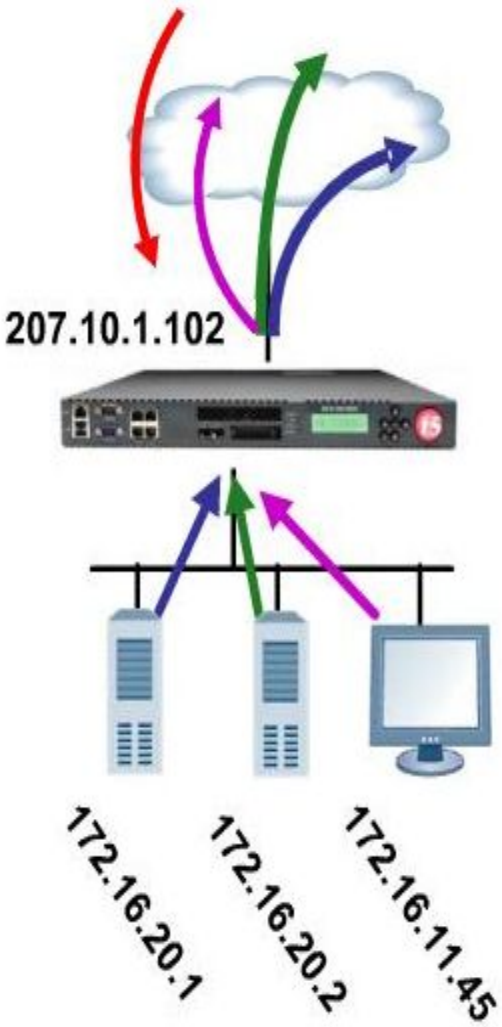
To resolve issue:

- **Servers default route**
- **Use SNAT**



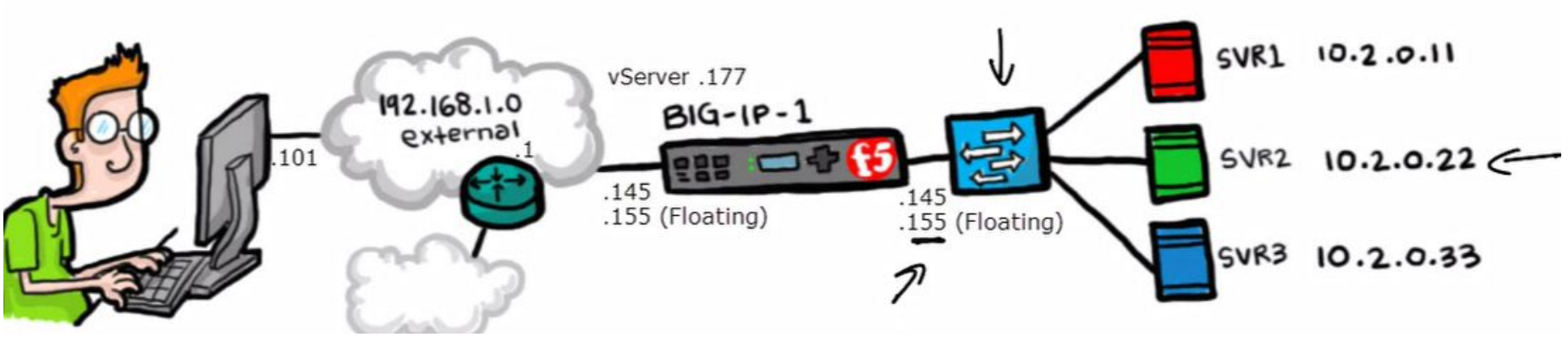
SNAT Concept

- “Secure” NAT
- Performs Source Nat
- Many to one mapping
- Traffic initiated to SNAT Address refused
- SNAT’s used for Routing problem



Auto Map

- Another approach for carrying out translation is Auto-Map
- In Auto-map communication would happen using the self-ip/Floating-ip of the device.
- F5 would here choose the interface depending the server subnet.



File System

- **Built on top Linux**
- **Has Linux files structure**
- **Files are relevant to the operation**
- **Main file in BIG-IP LTM are mentioned below:**

-/config/bigip.conf
-/config/bigip_base.conf
-/config/BigDB.dat
-/etc/hosts.allow
-/config/bigip.license
-/var/log/ltm

- **/config/bigip.conf**

- Holds all information relevant to the load balancing

Like: virtual, pool, profile, monitor, irules etc

-Shared between 2 units if in a pair configuration

- **/config/bigip_base.conf**

-Holds all information relevant to the basic elements of the BigIP

Like: management IP, vlans, routes few more things

- **/etc/hosts.allow**

-hosts which are allowed to use the local INET services.

Such as services are SSH, snmp for the snmp devices

- **/config/BigDB.dat**

-bigdb database holds a set of bigdb configuration keys

-Keys define the behaviours 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.

-We can edit these values by using

-The Configuration utility

-The bigpipe db command

#bigpipe db all list

- **/config/bigip.license**

-Holds all information about the license of the BigIP system

-Without this file or a valid license file, the BigIP will not operate

- **There are few more vital files**

/config/ssl/ssl.crt

/config/ssl/ssl.key

Chapter 10

iRule

What is an iRule?

- An iRule is a TCL script to give more control over how traffic is processed via the LTM
- Can do this based on just about anything found in a packet, including client IP address, headers, URI, destination port, etc.
- The use of the Universal Inspection Engine (UIE) is also done via iRules, allowing for rule based persistence

What can an iRule work with?

- Most commonly seen are HTTP events
- Can also work with other protocols, such as SIP, RTSP, XML, others
- Can make adjustments to TCP behavior, such as MSS, checking the RTT, looking into the payload
- Can work with authentication or encryption, via x509 commands, and AES encryption/decryption
- Cache, compression, profiles are also available

Sequence of Events

. client selected/accpeted:3 HS and then client is accepted
. http request:request made by client
. lb selected: selects lb
. server connected
. http response
.client closed-fin
. server closed

Example iRules

Change server headers

```
when HTTP_RESPONSE {
    HTTP::header replace Server "Microsoft-IIS/5.1"
}
```

Remove all server headers

```
when HTTP_RESPONSE {
    HTTP::header sanitize ?ETag? ?Header01? ?Header02?
}
```

On 404 error, re-load balance

```
when HTTP_REQUEST {
    set RequestedPage [HTTP::uri]
}
when HTTP_RESPONSE {
if { [HTTP::status] eq "404" } {
    log "Dooh, page '$RequestedPage' not found on server [IP::server_addr]!"
    HTTP::redirect $RequestedPage
}
}
```

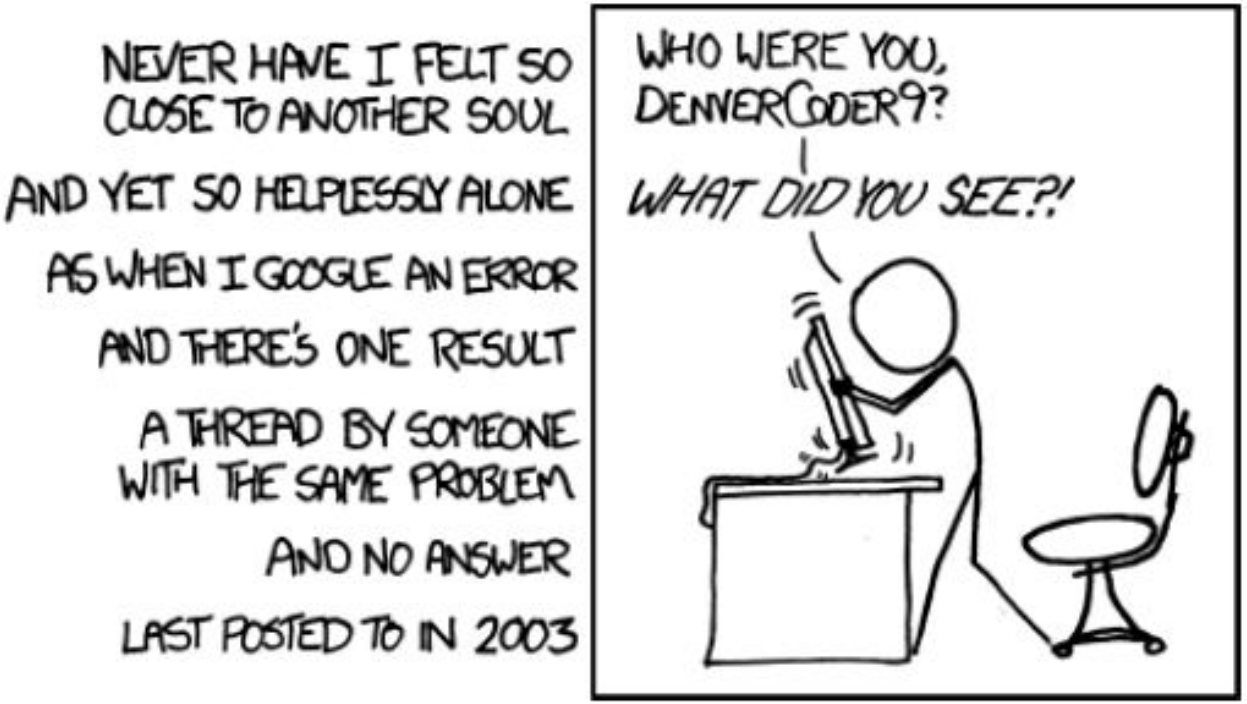
iRule Logging (really handy!)

- You can turn on logging for any iRule and record anything you like from requests or responses!
- Often used when troubleshooting an iRule
- Simply add the line "log xxx" (where "xxx" is anything you like) to any iRule, for example:

```
when HTTP_REQUEST {
log "Client [IP::remote_addr] has requested page
  [HTTP::uri] from server [HTTP::host]."
}
```

- You can use the CLI command "tail –f /var/log/ltm" to view these logs in real time

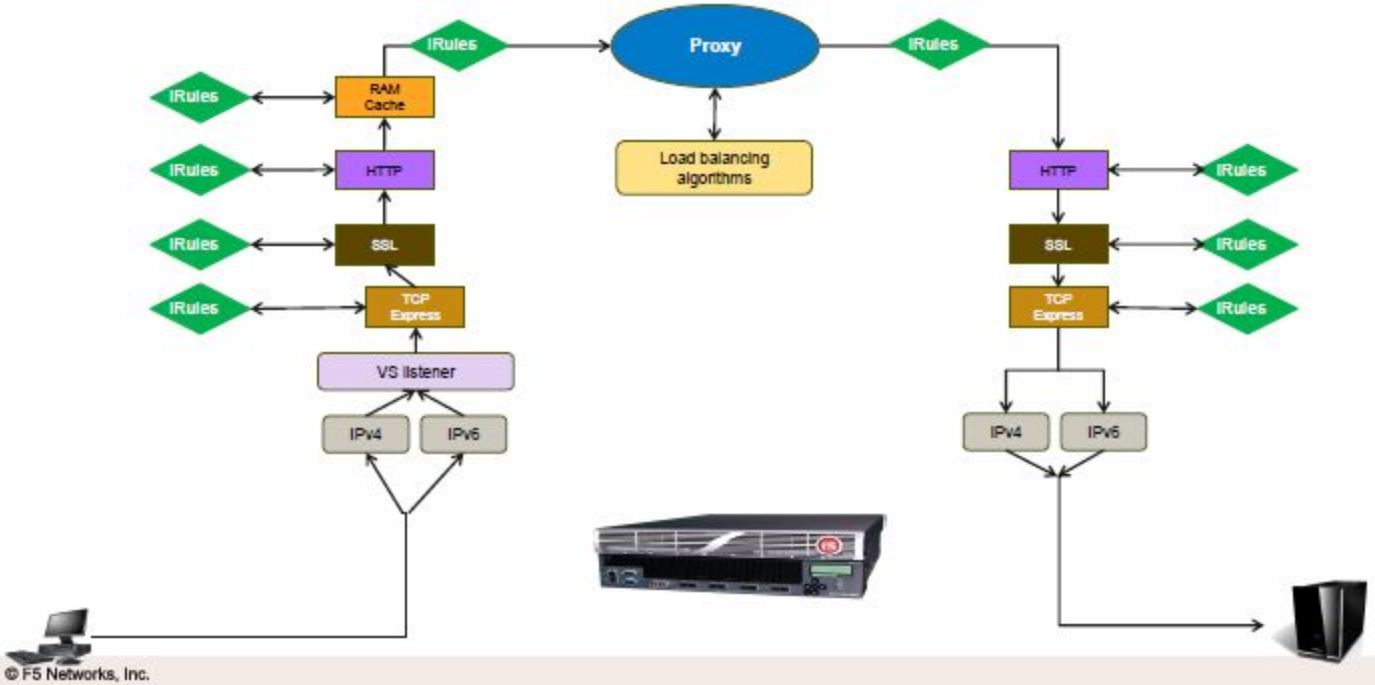
Troubleshooting

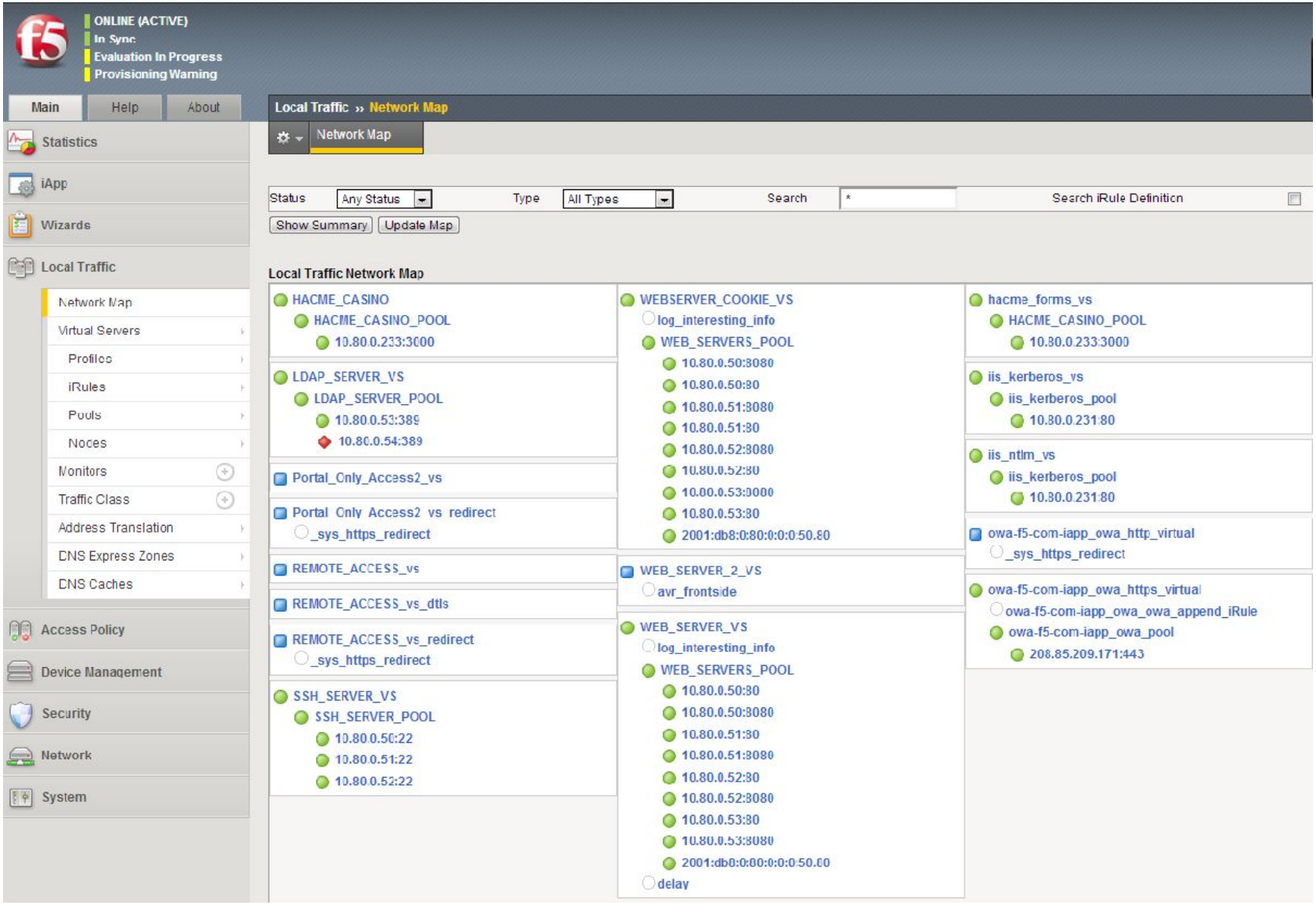


What are we troubleshooting?

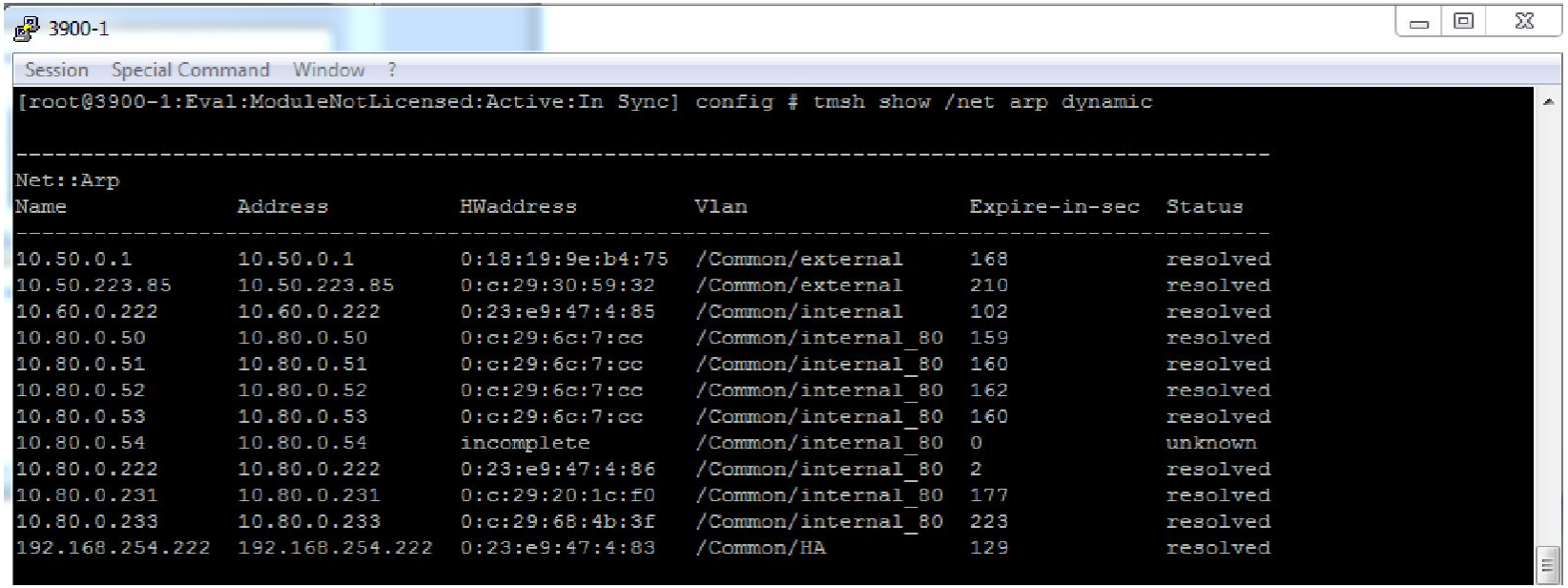
- Did this work before?
- Does the traffic go through the F5?
- Is it reproducible?
- Is there a log server?
- Did the timing of the issue coincide with any other changes?
- Before beginning determine what devices are involved
- Obtain or create a network diagram from the client to the F5 to the pool members

Standard Virtual Server Packet Flow




ONLINE (ACTIVE)
In Sync
Evaluation In Progress
Provisioning Warning
Main
Help
About
Local Traffic ›› Network Map
Statistics
iApp
Wizards
Local Traffic
Network Map
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
Traffic Class
Address Translation
DNS Express Zones
DNS Caches
Access Policy
Device Management
Security
Network
System
Network Map
Status
Any Status
Type
All Types
Search
*
Search iRule Definition
Show Summary
Update Map
Local Traffic Network Map
HACME_CASINO
HACME_CASINO_POOL
10.80.0.233:3000
LDAP_SERVER_VS
LDAP_SERVER_POOL
10.80.0.53:389
10.80.0.54:389
Portal_Only_Access2_vs
Portal_Only_Access2_vs_redirect
_sys_https_redirect
REMOTE_ACCESS_vs
REMOTE_ACCESS_vs_dtls
REMOTE_ACCESS_vs_redirect
_sys_https_redirect
SSH_SERVER_VS
SSH_SERVER_POOL
10.80.0.50:22
10.80.0.51:22
10.80.0.52:22
WEBSERVER_COOKIE_VS
log_interesting_info
WEB_SERVERS_POOL
10.80.0.50:8080
10.80.0.50:80
10.80.0.51:8080
10.80.0.51:80
10.80.0.52:8080
10.80.0.52:80
10.80.0.53:8080
10.80.0.53:80
2001:db8:0:80:0:0:0:50:80
WEB_SERVER_2_VS
avr_frontside
WEB_SERVER_VS
log_interesting_info
WEB_SERVERS_POOL
10.80.0.50:80
10.80.0.50:8080
10.80.0.51:80
10.80.0.51:8080
10.80.0.52:80
10.80.0.52:8080
10.80.0.53:80
10.80.0.53:8080
2001:db0:0:00:0:0:0:50:00
delay
hacme_forms_vs
HACME_CASINO_POOL
10.80.0.233:3000
iis_kerberos_vs
iis_kerberos_pool
10.80.0.231:80
iis_ntlm_vs
iis_kerberos_pool
10.80.0.231:80
owa-f5-com-iapp_owa_http_virtual
_sys_https_redirect
owa-f5-com-iapp_owa_https_virtual
owa-f5-com-iapp_owa_owa_append_iRule
owa-f5-com-iapp_owa_pool
208.85.209.171:443

tmsh show /net arp dynamic



- Ping
- Check routes
- Tracepath utility
- Traceroute from both directions
- Telnet to the remote port

```
[root@3900-1:Active:In Sync] config # tracepath
10.0.180.1
1: 10.50.0.221 (10.50.0.221) 0.175ms pmtu 1500
1: 10.0.180.1 (10.0.180.1) 2.981ms reached
Resume: pmtu 1500 hops 1 back 1
```

```
tmsh show /sys connection cs-server-addr 10.10.1.100
```

..might produce output similar to the following:

cs-client-addr:port	cs-server-addr:port	ss-client-addr:port	ss-server-addr:port
10.10.1.30:3378	10.10.1.100:22	10.10.1.30:3378	172.16.20.1:22 tcp 9
10.10.2.30:4599	10.10.1.100:22	10.10.2.30:4599	172.16.20.2:22 tcp 2

Running TCPDUMP

- TCPDUMP is an inbuilt network sniffer
- To run TCPDUMP from the CLI and save the output to a file that can be opened in Ethereal/Wireshark use the following command:

  tcpdump -ni <VLAN> -v -s 1600 -w /var/tmp/filename.dmp

  Example:

  tcpdump -ni external -v -s 1600 -w /var/tmp/external.dmp

- TIP: Use WinSCP to copy the file from the BIG-IP to your PC
- TCPDUMP can be run from the GUI also

Running SSLDUMP

- SSLDUMP is a utility available on the BIG-IP that can be used to decode your SSL sessions by pre-loading your SSL keys and using those to convert the session data into ASCII text.
- SSLDUMP takes a raw TCPDUMP file as input
- To display the handshake only
  - ssldump –r <capture file>
- To display the actual application data (with the key file)
  - ssldump –r <capture file> -k <key file> -d
  - Example:
    ssldump -r /var/tmp/internal.dmp -k /config/ssl/ssl.key/default.key -d > /var/tmp/ssldump.dmp
- Documentation for ssldump can be found on www.rtfm.com/ssldump/ssldump.html

Logs

- Logs can often highlight problems
- Can be viewed from the GUI
- Can be downloaded from the directory "/var/log"
- Useful command to watch the LTM log file in real time from the CLI:

  tail –f /var/log/ltm

“Qkview”

- Support will often request these
- Can be executed from the GUI or CLI
- Contains box configuration, route information, statistics etc

Useful links… F5 related

- Compression Test
  - http://www.f5demo.com/compression
- Devcentral (iRules, iControl, SDK)
  - http://devcentral.f5.com
- Software Downloads
  - http://downloads.f5.com
- Askf5 (manuals, software, solutions, EOL info)
  - http://www.askf5.com

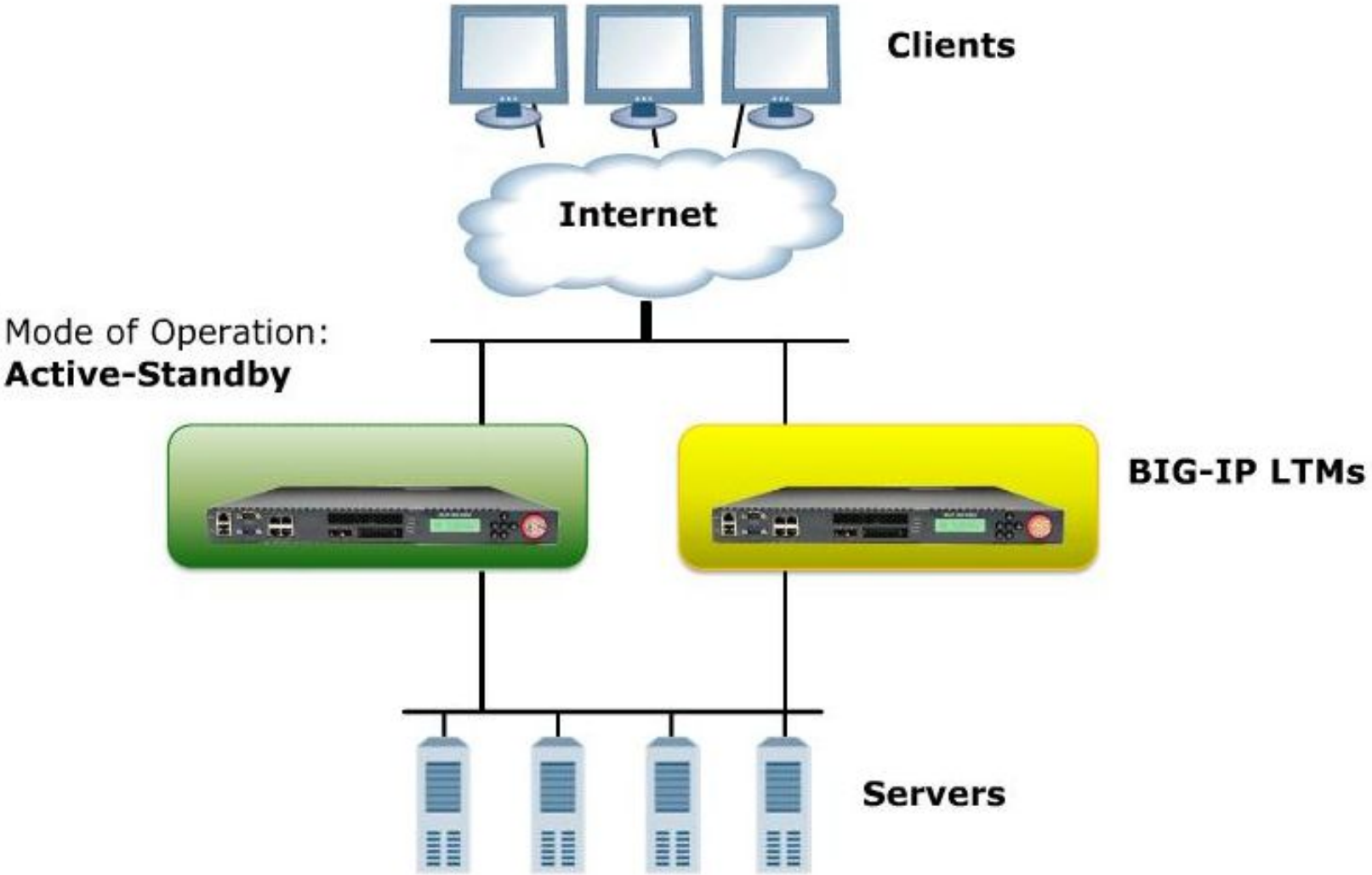
Chapter 11

Redundant Pair

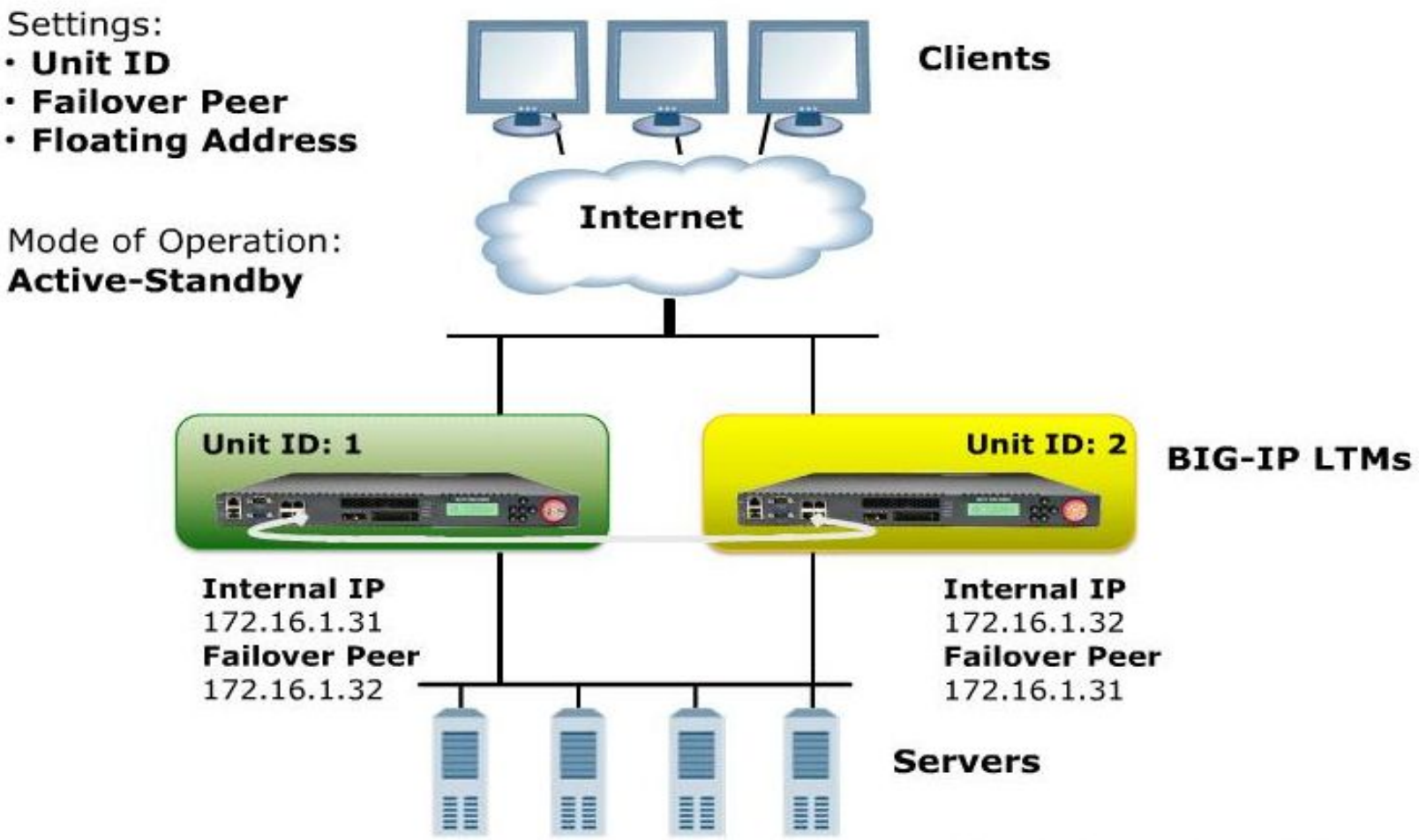
- *Redundant pair Concept*
- *Redundant Pair Setup*
- *Config. Synchronization*

Concept..

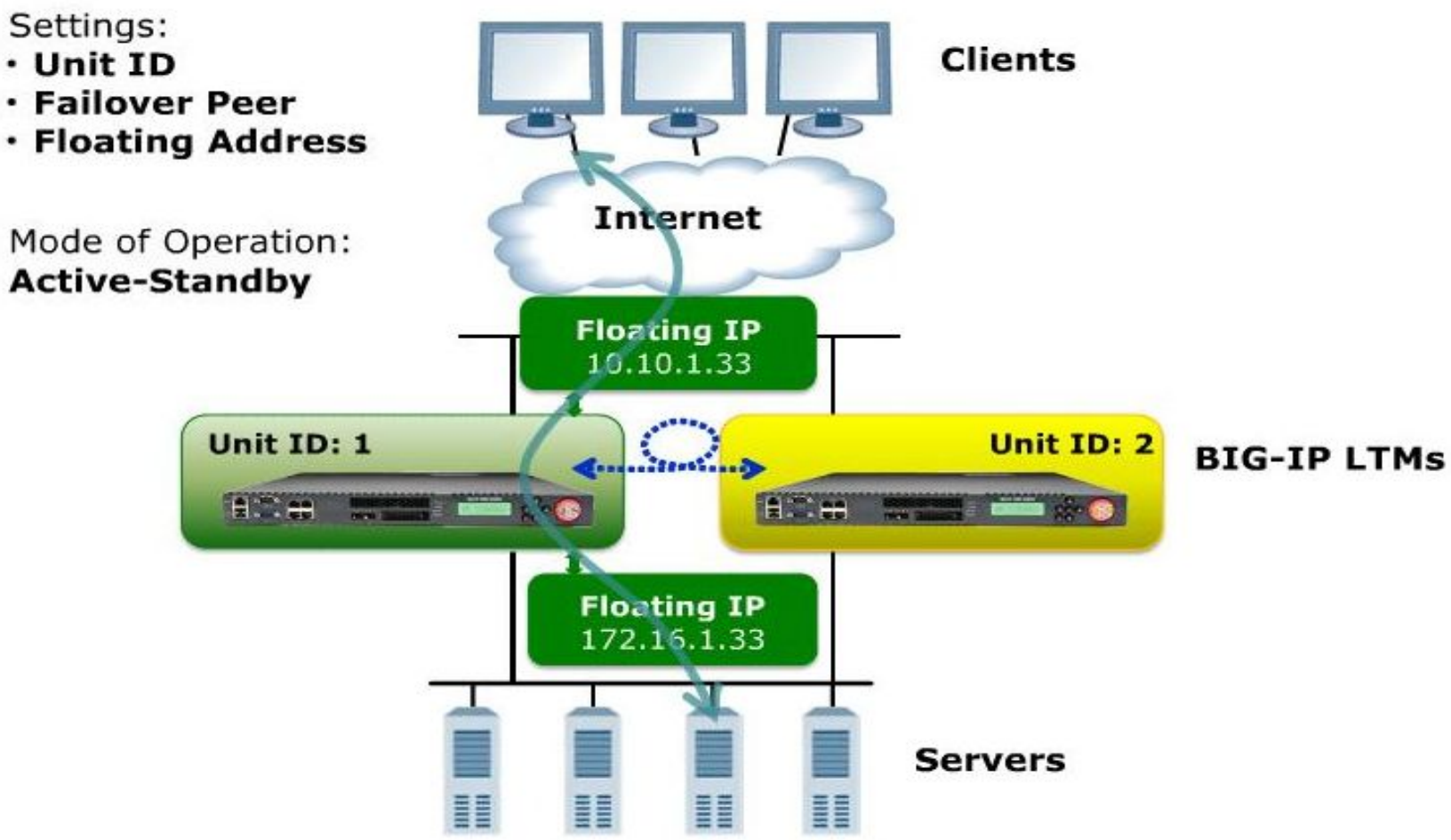
- When is high Availability is required ?
  - ☐Increases Reliability
  - ☐It consist of two identically configured Big-IP system
- There are two basic aspect:
  - ☐Synchronizing configurations between two BIG-IP units
  - ☐Configuring fail-safe settings for the VLANs


Clients
Internet
Mode of Operation:
Active-Standby
BIG-IP LTMs
Servers

- Unit ID used for Identification, do not designate primary and secondary

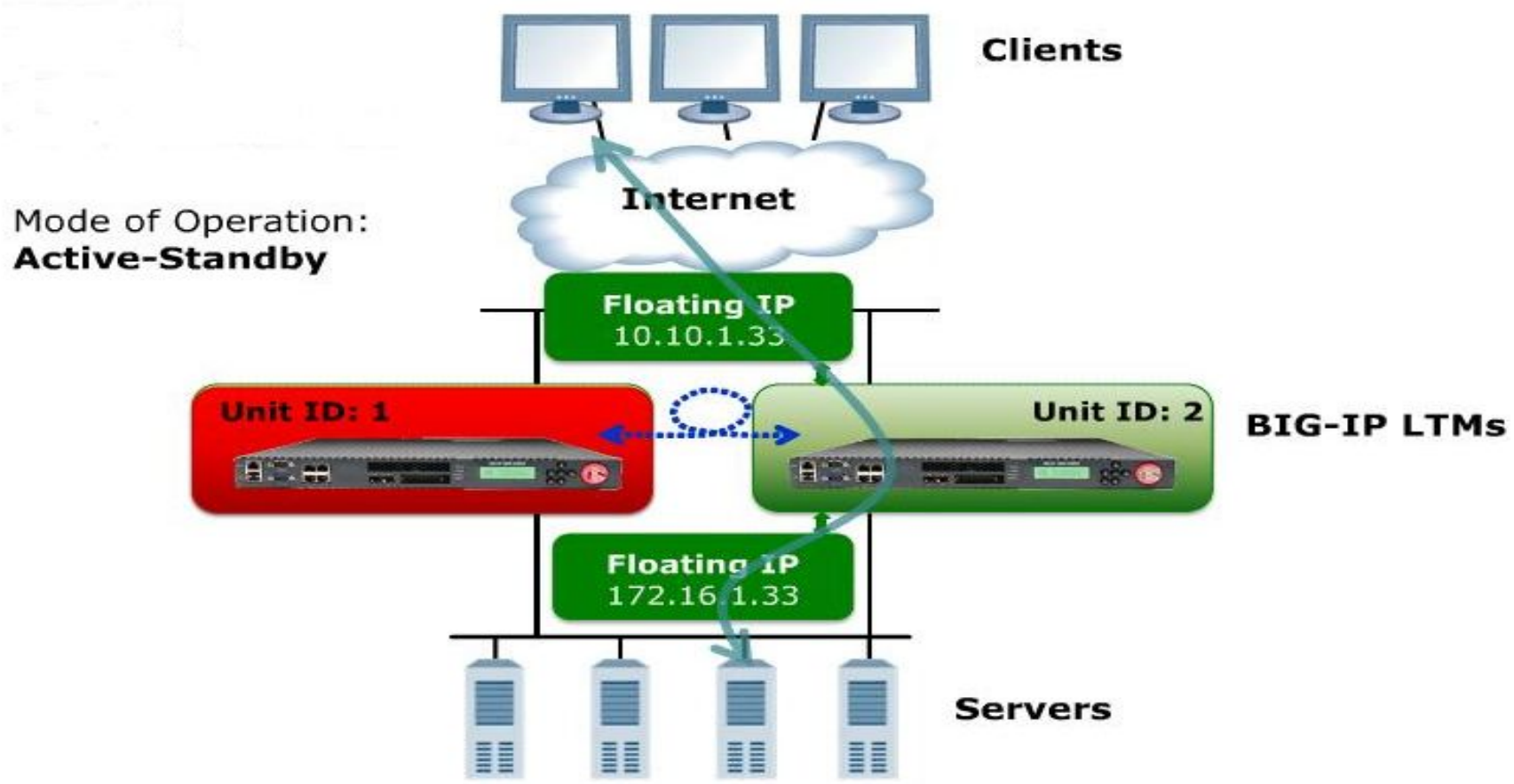


- Floating IP is always own by Active box

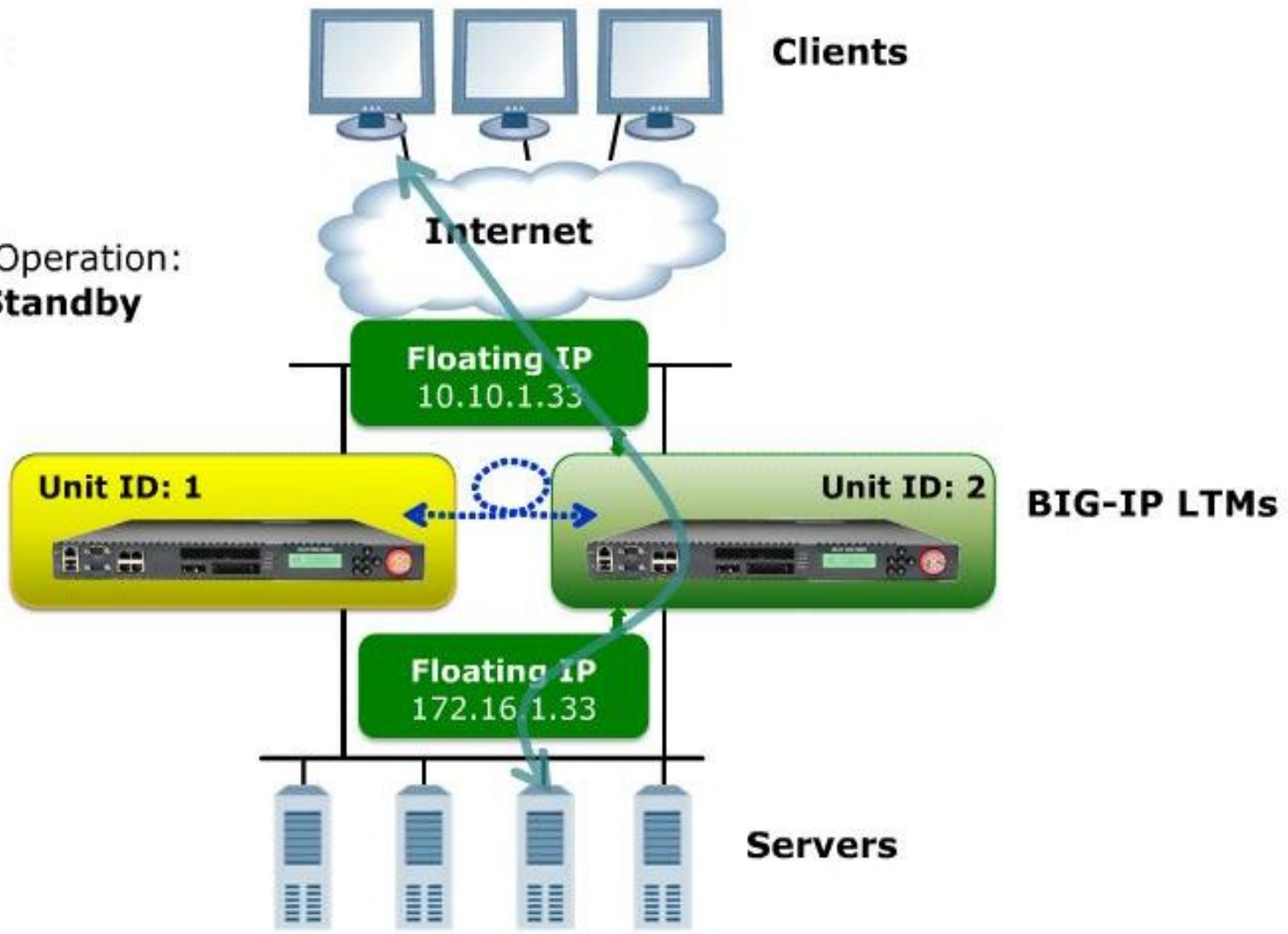


Failing Over

>Gratuitous ARP sent to all neighboring network devices

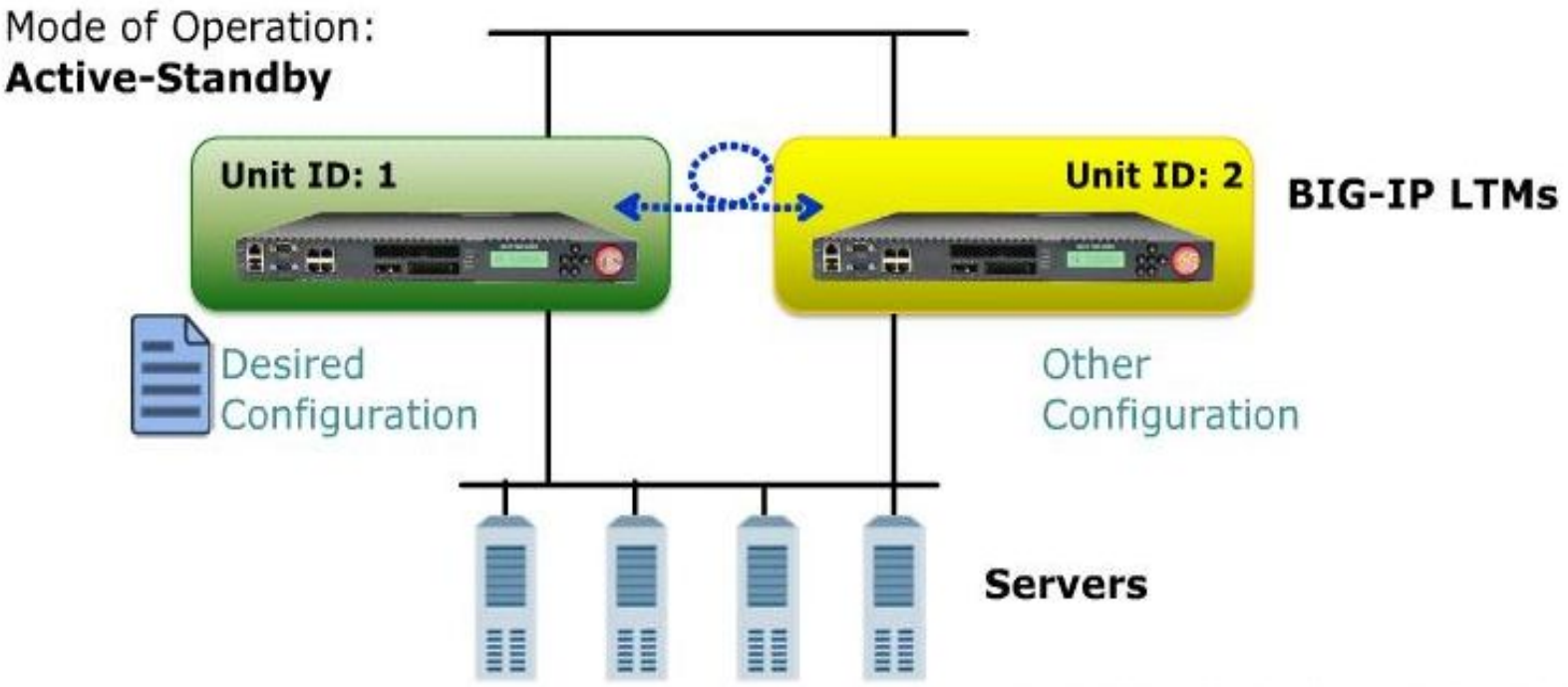


Mode of Operation:
Active-Standby



Synchronize Configuration

- Initiated from Either System
- Redundant pair should service the same monitors, pools & virtual Servers



Synchronization condition

- Administrative password must be same on each system
- Port 443 must not be blocked by the port lockdown setting or by another system between the redundant pair.
- Clock of the system must be within a certain number of minutes of each other.
- Pull or Push Operation –Sync in Correct Direction

Synchronization Process

1-Create UCS file.

-Which contain all configurations + licensing information

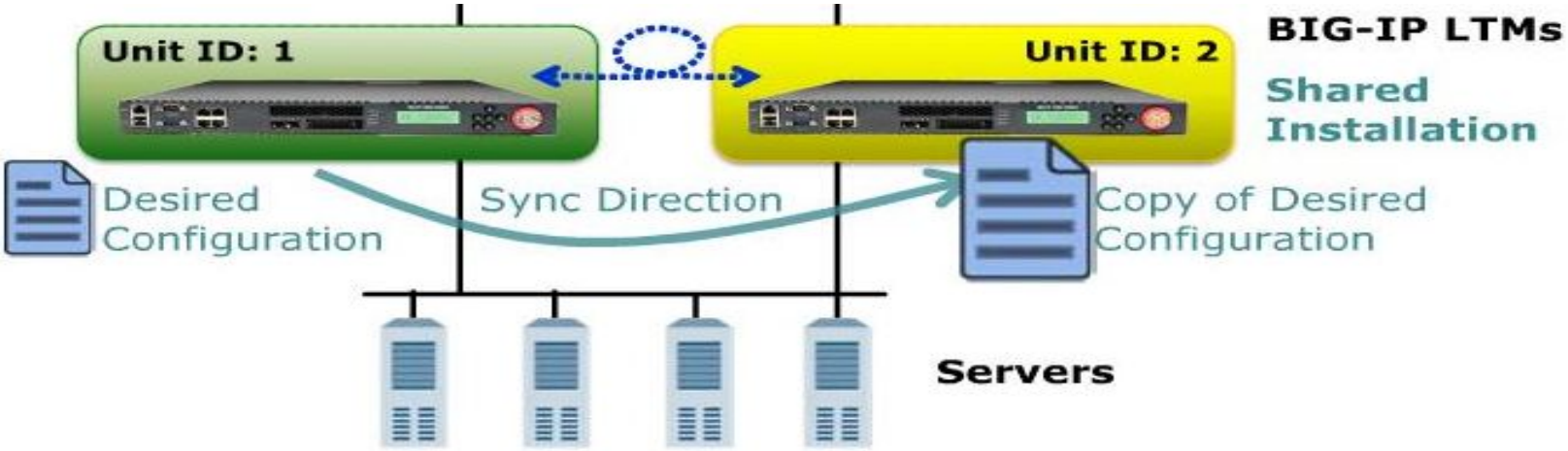
2-Send to peer

3-Peer creates backup of itself

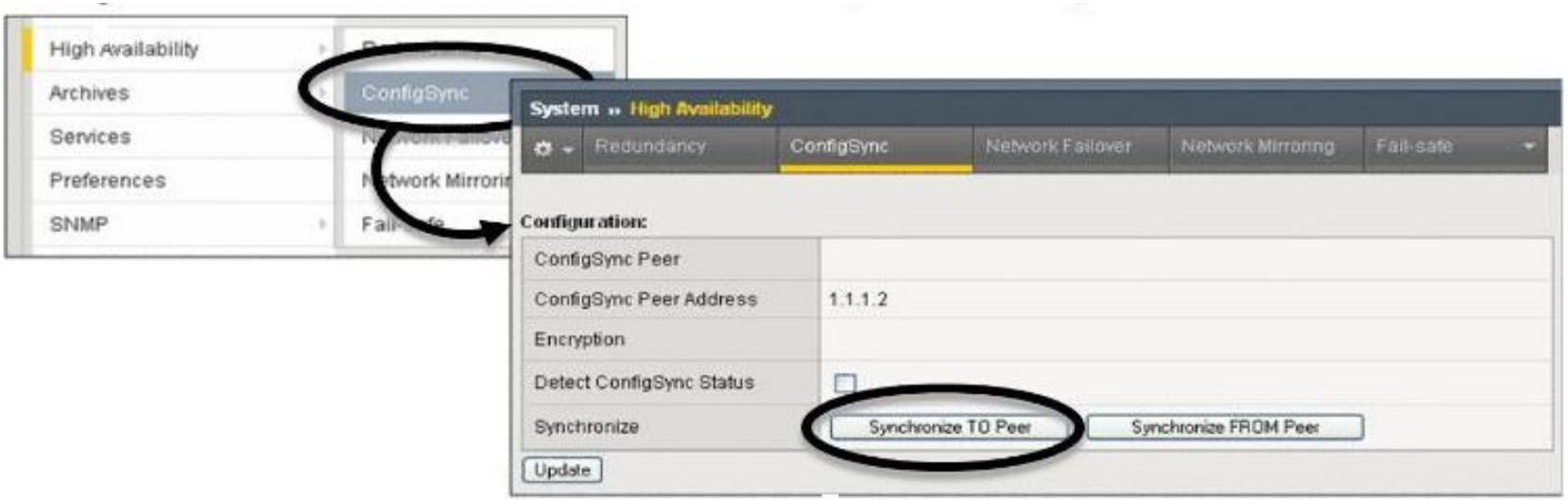
4-Peer opens UCS file

a) Matching Hostname > Full Installation

b) Different Hostname >Shared Installation



Synchronize to Peer



Determine Active System

Change to Standby Mode

Chapter 12

High Availability

- *Failover Trigger*
- *Failover Detection*
- *Stateful Failover*

Failover Managers

- Failover Mangers detects a failed process,
- takes one of the several action restarting the process, failing back to the standby, reboot the big-ip
- Watchdog
  - Performs hardware health checks
- Overdog
  - Software to correct hardware failures
- SOD
  - monitors the switch fabric and takes corrective action for switch failures

All failover Managers update and monitor the high Availability Table

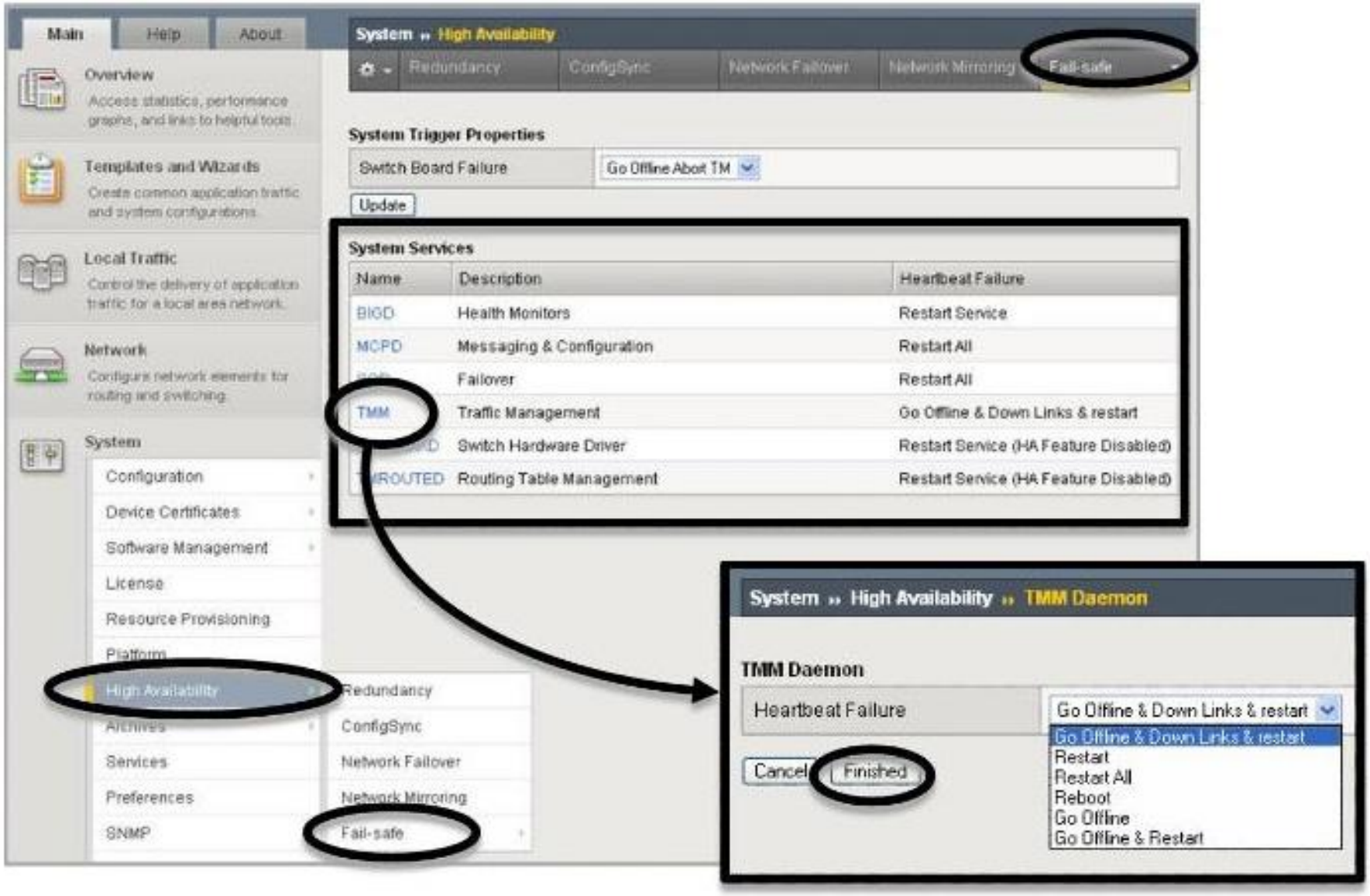
Failover Trigger

- Processes (Daemons)
- Switchboard
- VLAN Failsafe
- Gateway Failsafe

System Services

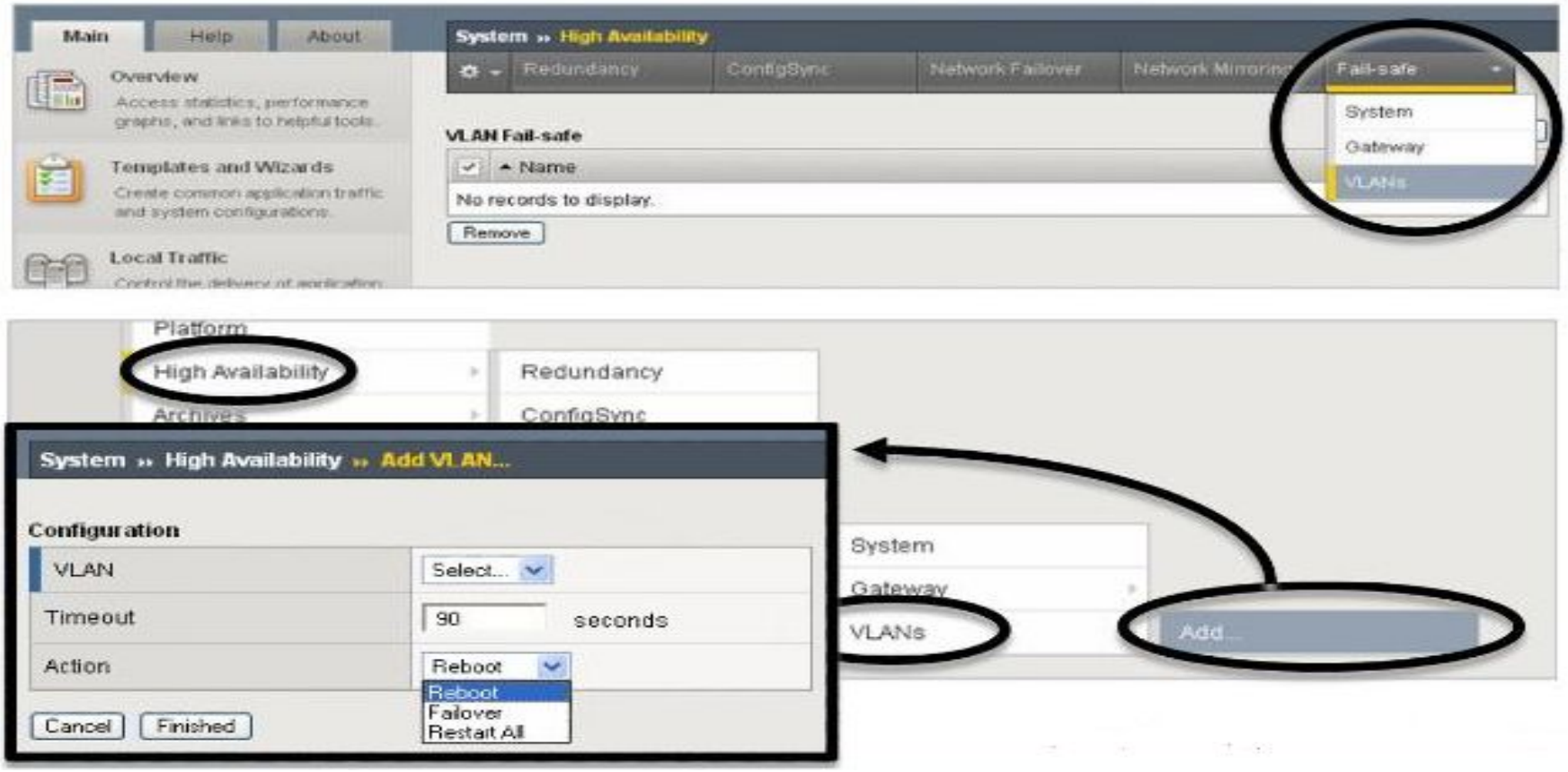
Name	Description	Heartbeat Failure
BIGD	Health Monitors	Restart Service
MCPD	Messaging & Configuration	Restart All
SOD	Failover	Restart All
TMM	Traffic Management	Go Offline & Down Links & restart
BCM56XXD	Switch Hardware Driver	Restart Service (HA Feature Disabled)
TMROUTED	Routing Table Management	Restart Service (HA Feature Disabled)

Failover Triggers - Daemons



VLAN Failsafe

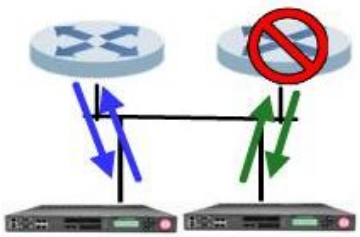
Virtual Local Area Network (VLAN) failsafe is a high availability (HA) feature that allows the BIG-IP system to monitor for network failure on VLANs and to take appropriate action when the system detects a loss of network connectivity.

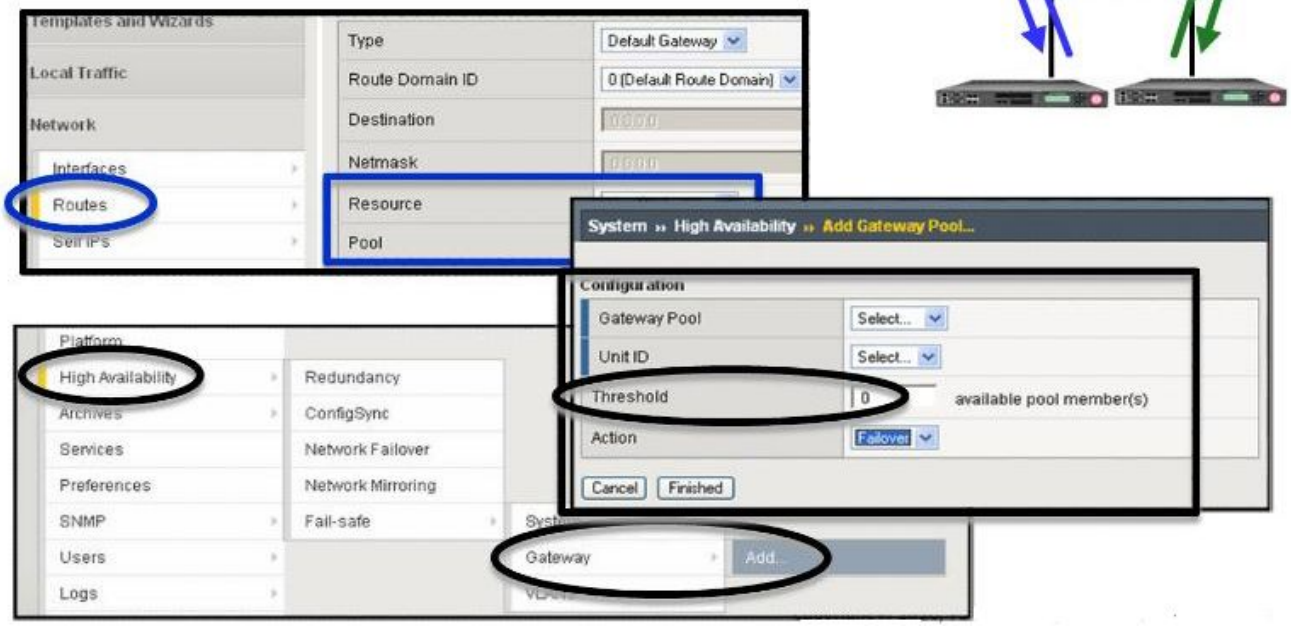


Gateway Failsafe

The gateway fail-safe feature allows further redundancy between BIG-IP device group members that point to different gateways. The gateway fail-safe feature allows each BIG-IP system to monitor the upstream gateway it uses to route traffic. If the gateway is marked down, the BIG-IP system can fail over to the next active device to prevent further disruption to traffic.

- Default Gateway Pool
- Number of Gateways below threshold

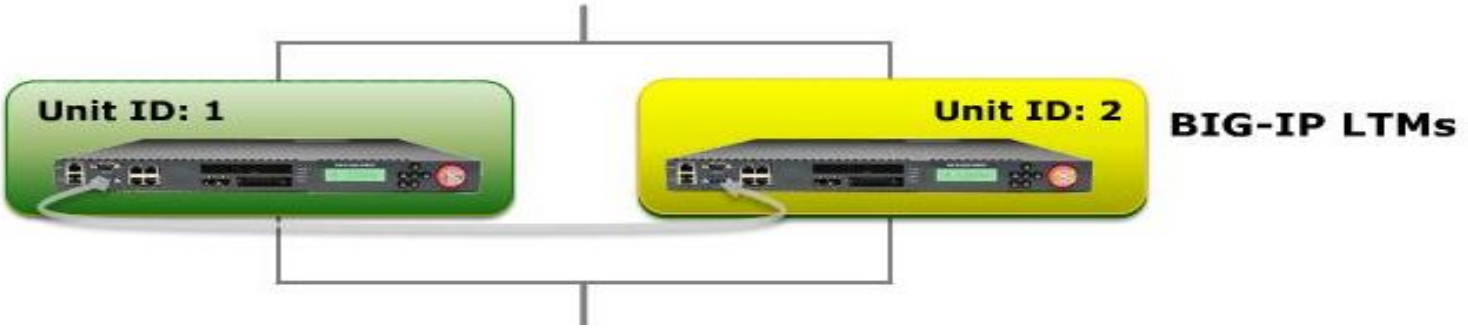




Hardware Failover

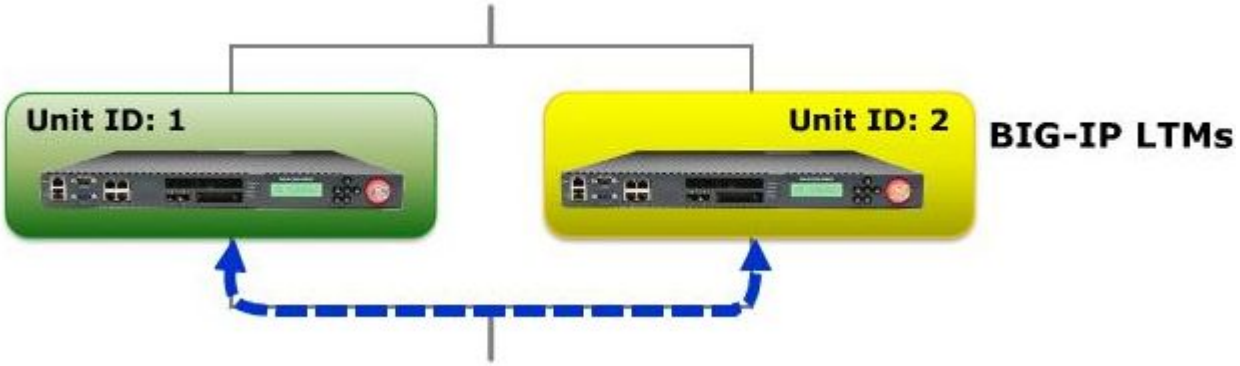
- Standby notices a loss of voltage, it Takes over the active role

- Always enabled
- Front Panel Failover Port to Port
- Failover Cable
  - Specially pinned DB9 cable
  - Active system applies voltage
  - Carries no data
  - Max. length: 50 feet (15.24 meters)

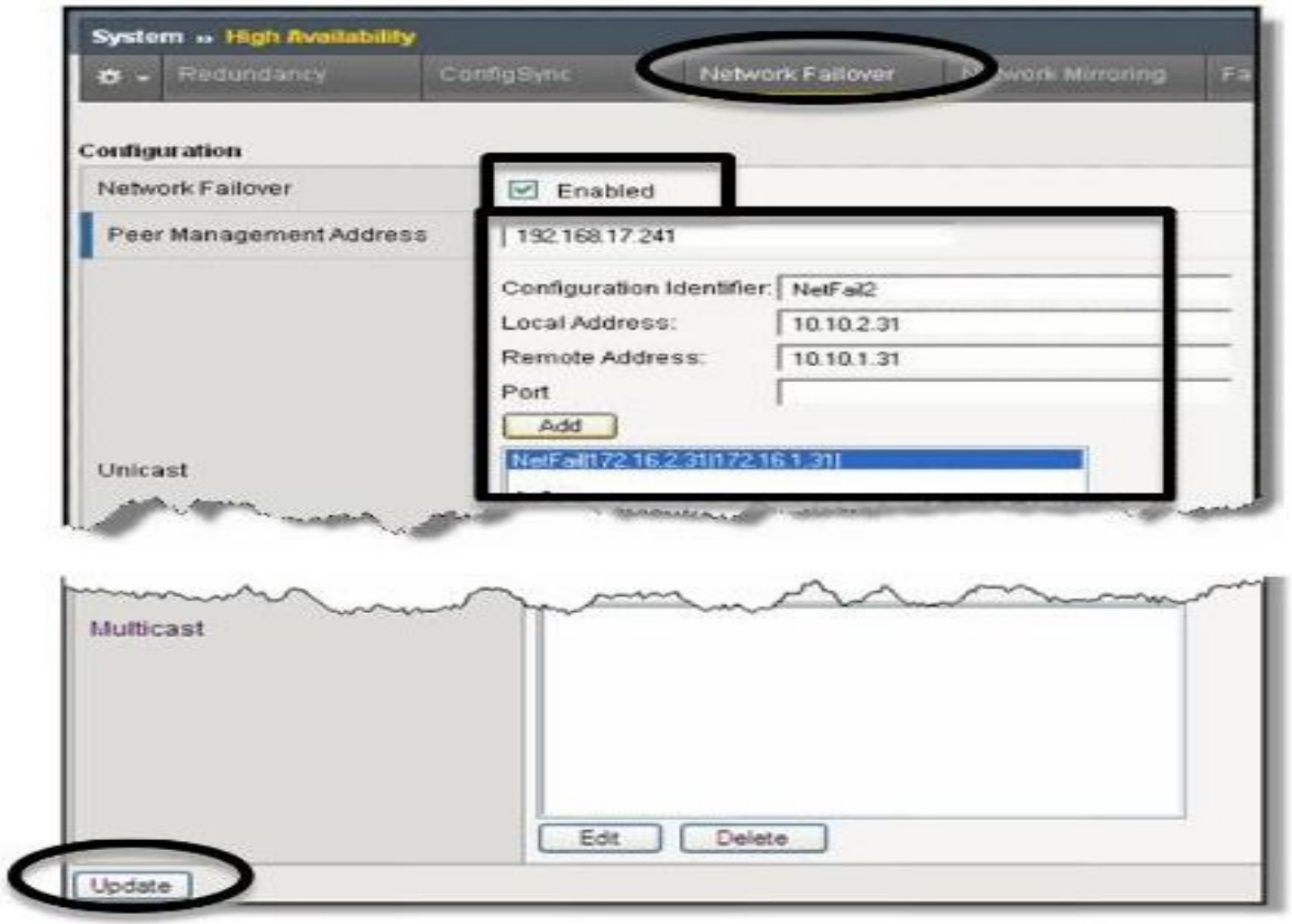


Network Failover

- Heartbeat sent over network
- No 50 foot (15.24 meter) limitation
- Slower than Hardware Failover
- Setting not synchronized between peers
- If Both Hardware Failover & Network Failover are being used.....

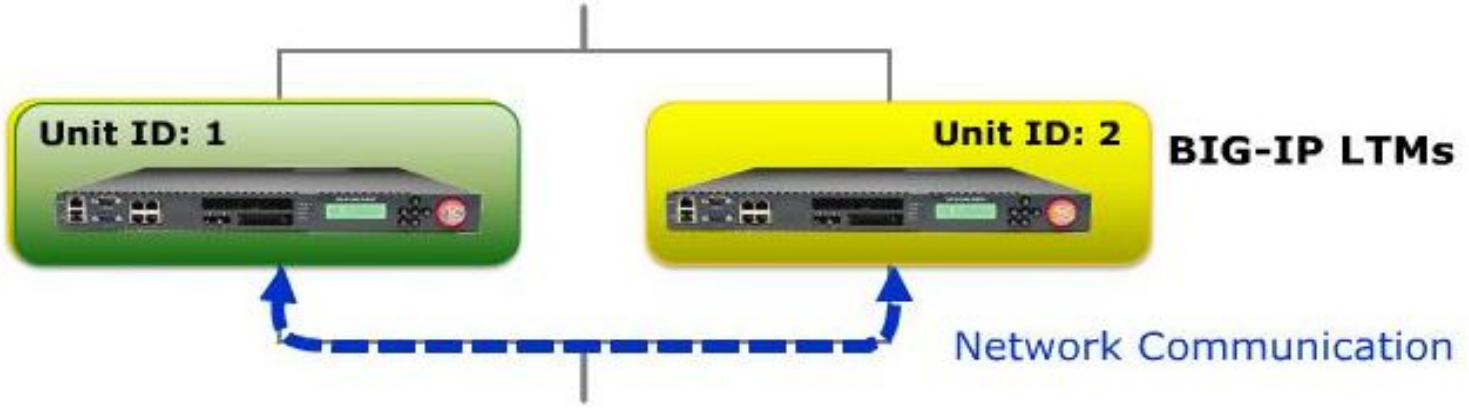


Network Failover Settings



Network Communication

- Synchronization Data:
  - TCP Connection – Port 443
  - Configuration Synchronized with Peer
- Network Failover:
  - UDP Datagrams – Port 1026
  - Network keep-alive when enabled
- Mirroring Data:
  - TCP Connection – Port 1028
  - Connection and Persistence Tables Mirrored when Enabled



Stateful Failover

- Default Actions on Failover
  - New connections through new Active system
  - Current connections and persistence lost
- Stateful Failover
  - New connections through new Active system
  - Current connections and persistence maintained
  - Accomplished by Mirroring data to Standby

Types of Mirroring

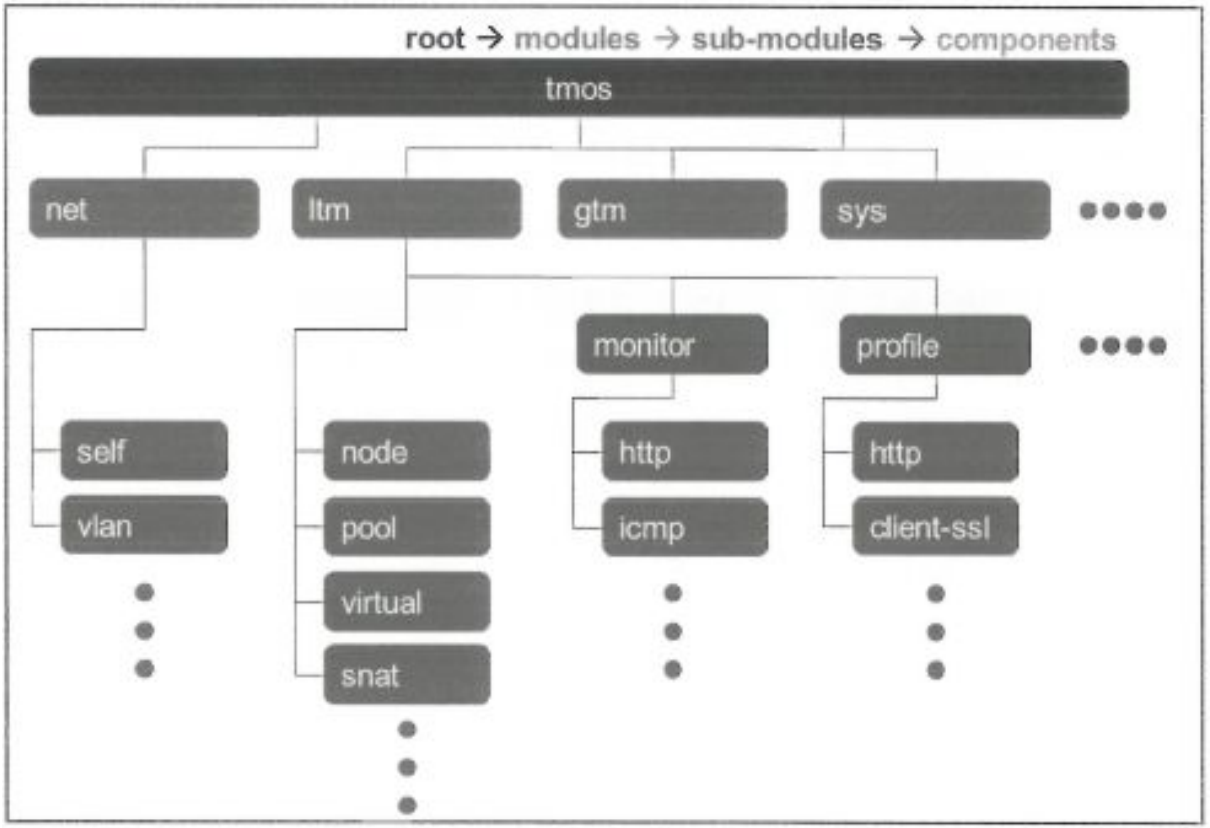
- Connection Mirroring
  - Applicable to Long Lasting connections like telnet, ftp, ssh, etc…
  - Connection should not be lost
- Persistence Mirroring
  - For Persistent sessions
  - Timer starts anew at Failover

Advance Topics

- CLI
- Partitions
- Route Domains

CLI- TMSH and
TMOS

- F5 GUI configuration is converted into CLI.
- Type of Prompt-Bash and TMSH
- TMSH- Traffic management shell which moves you to TMOS(Traffic Management Shell) used for device management.
- Its hierarchy based structure with TMOS on top and then followed by Modules, Sub modules and Components
- Modules: Depending upon Licensing and provisioning the modules that will be available-auth,cli,ltm,gtm,network,system
- Submodules: This would contain submodules of modules like LTM has profile,monitor.
- Components:Actual objects configured on BIG-IP – Node,pool,vlan



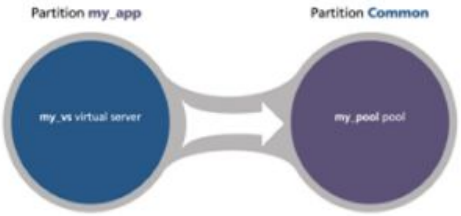

```
[root@bigip4:Active:Standalone] config # tmsh          ← Enter
root@(bigip4)...(tmos)# ltm pool                       ← Dive
root@(bigip4)...(tmos.ltm.pool)# exit                  ← Up 1 level
root@(bigip4)...(tmos.ltm)# /net vlan                  ← Traverse
root@(bigip4)...(tmos.net.vlan)# /                     ← To tmos root
root@(bigip4)...(tmos)# quit                           ← Exit
[root@bigip4:Active:Standalone] config #
```

Partitions

- Partitions are similar to context where you can assign objects and control their visibility, management to objects.
- If you have the Administrator or User Manager user role assigned to the BIG-IP system user account, you can create administrative partitions to control other users' access to BIG-IP objects.

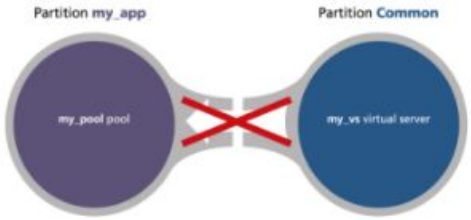
- By Default the partition is Common, all the entities created are stored in Common partitions.
- Object movement is not possible to other partitions you need to delete them and create them into partition.
- Administrators have full control over the data.A user defined for that particular partition will only have rights for modification for that partition only, they can view content of common partition.
- For objects in partitions

Another valid object referencing case is when the object resides in one partition, while the object it references resides in partition `Common`. This figure shows an example of this configuration, where a virtual server in partition `my_app` references a pool in partition `Common`:



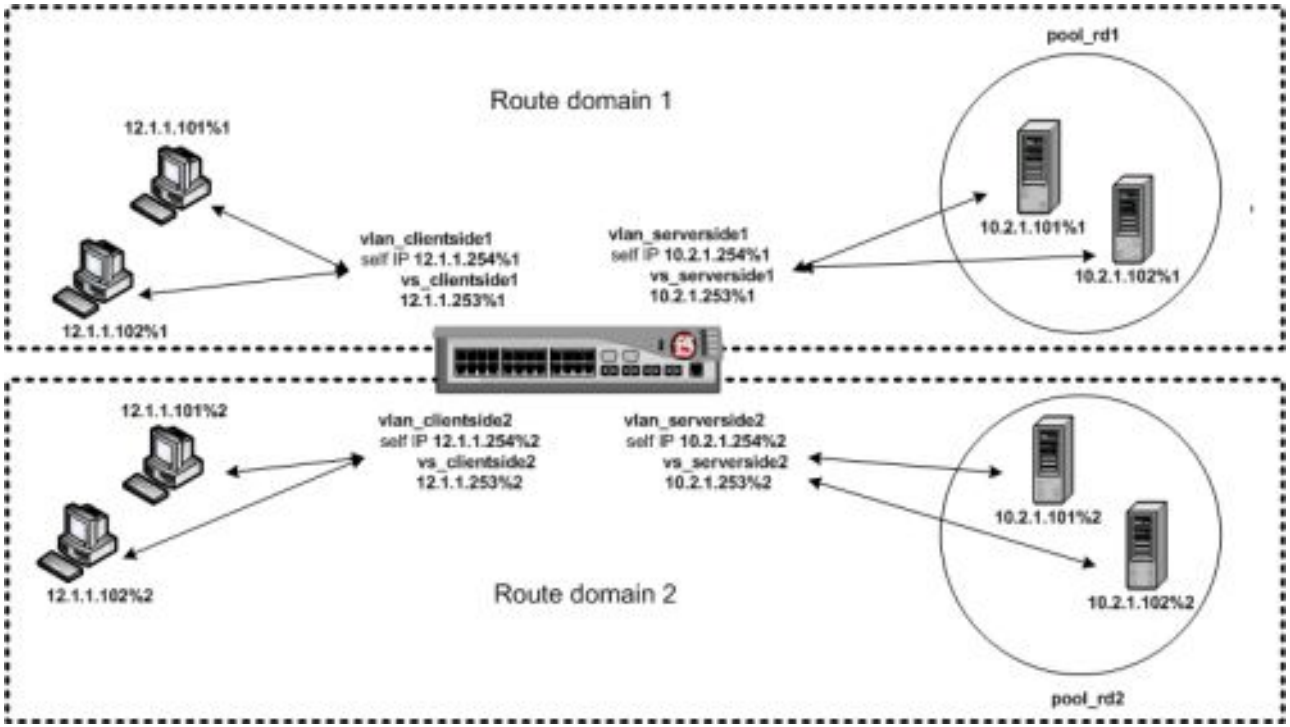
Invalid object referencing

This figure shows an example of an invalid object-referencing configuration, where a virtual server resides in partition `Common`, but the pool the virtual server references resides in a different partition. In this case, the virtual server cannot successfully forward traffic to the pool that it is referencing:



Route Domain

- A route domain is a configuration object that isolates network traffic for a particular application on the network.
- Because route domains segment network traffic, you can assign the same IP address or subnet to multiple nodes on a network, provided that each instance of the IP address resides in a separate routing domain
- Using the route domains feature of the BIG-IP system, you can provide hosting service for multiple customers by isolating each type of application traffic within a defined address space on the network.
- With route domains, you can also use duplicate IP addresses on the network, provided that each of the duplicate addresses resides in a separate route domain and is isolated on the network through a separate VLAN


pool_rd1
Route domain 1
12.1.1.101%1
12.1.1.102%1
vlan_clientside1
self IP 12.1.1.254%1
vs_clientside1
12.1.1.253%1
vlan_serverside1
self IP 10.2.1.254%1
vs_serverside1
10.2.1.253%1
10.2.1.101%1
10.2.1.102%1
12.1.1.101%2
12.1.1.102%2
vlan_clientside2
self IP 12.1.1.254%2
vs_clientside2
12.1.1.253%2
vlan_serverside2
self IP 10.2.1.254%2
vs_serverside2
10.2.1.253%2
10.2.1.101%2
10.2.1.102%2
Route domain 2
pool_rd2

- A route domain ID is a unique numerical identifier for a route-domain. You can assign objects with IP addresses (such as self IP addresses, virtual addresses, pool members, and gateway addresses) to a route domain by appending the %ID to the IP address.

- The format required for specifying a route domain ID in an object's IP address is A.B.C.D%ID, where ID is the ID of the relevant route domain **10.10.10.30%2 pertain to route domain 2**
- The BIG-IP system includes a default route domain with an ID of 0.
- Traffc flow between different route domain can be controlled via strict isolation where the RD remains to that partition.
- Forwarding of traffic between route domains is by default enabled between route domains in a parent-child relationship only. (That is, traffic received in a child route domain can be forwarded to a parent route domain and the reverse.)
- Each route domain can have a parent route domain, identified with a parent ID. ***The parent ID*** identifies another route domain on the system that the system can search to find a

- For example, suppose you create route domain 1 with a parent ID of 0. For traffic pertaining to route domain 1, the system looks within route domain 1 for a route for the specified destination. If no route is found, the system searches the routes in route domain 0.
- If the system finds no route in the parent route domain, the system searches the parent route domain's parent, and so on, until the system finds either a match or a route domain with no parent.
- The BIG-IP system, by default, includes one route domain, named route domain 0. Route domain 0 is known as the default route domain on the BIG-IP system, and this route domain resides in administrative partition Common. If you do not create any other route domains on the system, all traffic automatically pertains to route domain 0.
- Else you can set the route domain as per the partition needed.

Questions?