Elfiq Link Balancer (Link LB)
Quick Web Configuration Guide

Elfiq Operating System (EOS) - Version 3.5.0 and higher

Document Version 2.0 -January 2012

Elfiq Networks (Elfiq Inc.)

www.elfiq.com

1. About the Document

Purpose

This document provides detailed information on configuring and managing Elfiq Link Balancer through the web GUI.

Conventions

In this document, the following conventions are used:

- Menu clicks directions syntaxes are written in `10pt Arial` on a single in bold:
  wizards and settings -> basic configuration menu
- Promptmessages are written in bold under cotes :
  "The commands have been sent to the Link Balancer"
-
- Specific annotations are written in **bold** and can be of 3 types:
  NOTE
  IMPORTANT
  WARNING

Additional Information

For online access to our complete set of documentation and tools, please visit the support section of our website at http://www.elfiq.com

Support Center

You can contact the Elfiq Support Center at support@elfiq.com or at +1-514-667-0611 option 2. A member of our team will be pleased to assist you.

© Copyright 2011-2012, Elfiq Networks (Elfiq Inc.). All rights reserved.

All the information contained in this document is owned by Elfiq inc. and protected by worldwide copyright laws. No modification or reproduction is permitted without the prior written authorization of the owner.

Elfiq is a trademark of Elfiq Inc. All trademarks mentioned herein belong to their respective owners.

Elfiq inc. shall not be liable for any damages resulting from the use of this information and the products described herein.

Elfiq inc. reserves the right to make changes to any information within this document and to make improvements and/or changes in the products described herein at any time and without notice.

Table of Contents

1. ABOUT THE DOCUMENT 2

2. INTRODUCTION 4

3. ACCESSING THE UNIT 6

4. BASIC SYSTEM CONFIGURATION 7

5. BASIC VIRTUAL FORWARDER INTERFACE (VFI) CONFIGURATION 11

5.1. Configuring the primary link 11

5.2. Add Link wizard 14

5.3. Load balancing configuration 17

5.3.1. IP association 17

5.3.2. Outgoing Load Balancing 24

5.3.3. Incoming Load Balancing 29

6. INSTALLATION 36

7. VERIFICATION 38

2. Introduction

In this guide, we will show you how to configurean Elfiq Link Balancer to load balance incoming and outgoing traffic, in an infrastructure with two internet providers. We will use the GUI interface to complete the setup[1].

We will take as an example the following information:

Elfiq model: LB550E

The primary[2] Link info is:

- Provider Name: Provider1_T1
- Link Type: T1
- Download Bandwidth (kb/s): 1544
- Upload Bandwidth (kb/s): 1544
- MTU Size (if known): 1500
- Provider's Router IP Address: 194.204.1.1
- Subnet Mask: 255.255.255.0

The secondary link is:

- Provider Name: Provider2_xDSL
- Link Type: DSL
- Download Bandwidth (kb/s): 5100
- Upload Bandwidth (kb/s): 820
- MTU Size (if known): 1492
- Provider's Router IP Address: 212.217.1.1
- Subnet Mask: 255.255.255.0

A DMZ configured with three servers

- Local DNS server IP address : 194.204.1.102
- A mail server IP address : 194.204.1.101
- A web server (http/https) IP address :194.204.1.100

A firewall with an IP address: 194.204.1.3

For the purpose of this tutorial we will, we will define some link balancing policies on the Link LB.

- Make all outgoing web traffic (http and https) to be load balanced equally on both links.
- Make incoming secured web (https) and email traffic to failover to a secondary link (Provider2_xDSL) if the primary goes down.

[1]This setup is based on scenario1 presented in the LinkLBConfigGuide. If you want to configure the Link LB with the command line interface (CLI), please refer to the enclosed CD; it contains a quick configuration guide using CLI. It also contains how to add advanced features like SitePathMTPX and GeoLink.Should you require more information regarding Link LB commands, administration and protocol specific information, please refer to the EOS Admin Guide

[2]Primary link is the original link prior to installing an Elfiq Link Balancer and it's IP addressing scheme is used to assign IP addresses in the network

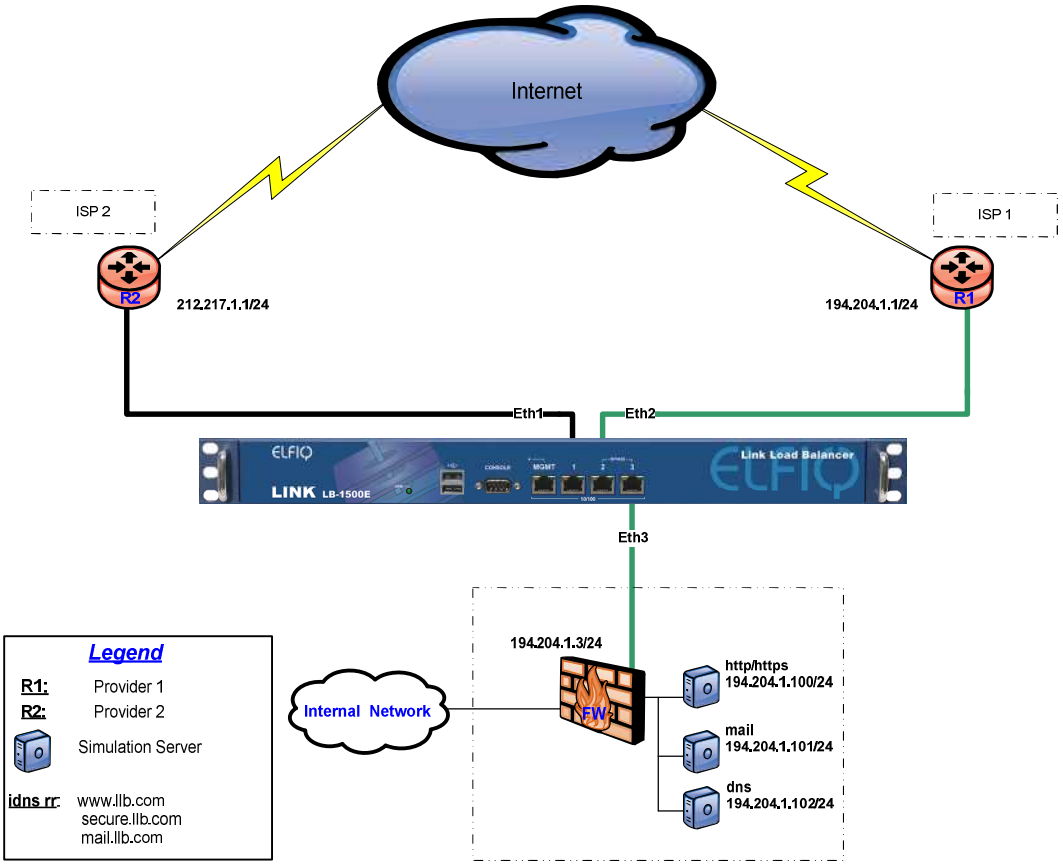


Figure 1

As shown in Figure 1, Elfiq link balancer will be installed between the firewall and the service provider

The primary link will be connected on port Eth2 and the firewall will be connected on port Eth3 of the Link LB. These are the Failsafe[3] ports by default in this model. The secondary link can be connected on any of the remaining ports; in our case, we used port Eth1.

[3]Always connect the primary Link and the firewall on the pair of ports shown as bypass on the front plate of the unit. Failsafe will bridge the two ports to keep the connection with the primary link if the Link LB goes down.

3. Accessing the unit

The Link LB has a dedicated management interface and can be accessed via SSH on port 22 or via the web interface on port 80.

1. Connect the Link LB unit power cord.
2. Connect the management interface to your computer.
3. Configure the Network interface of your computer with 10.1.0.x/24[4].
4. Start your web browser and navigate to the unit's IP address (by default 10.1.0.100).

The default credentials are:

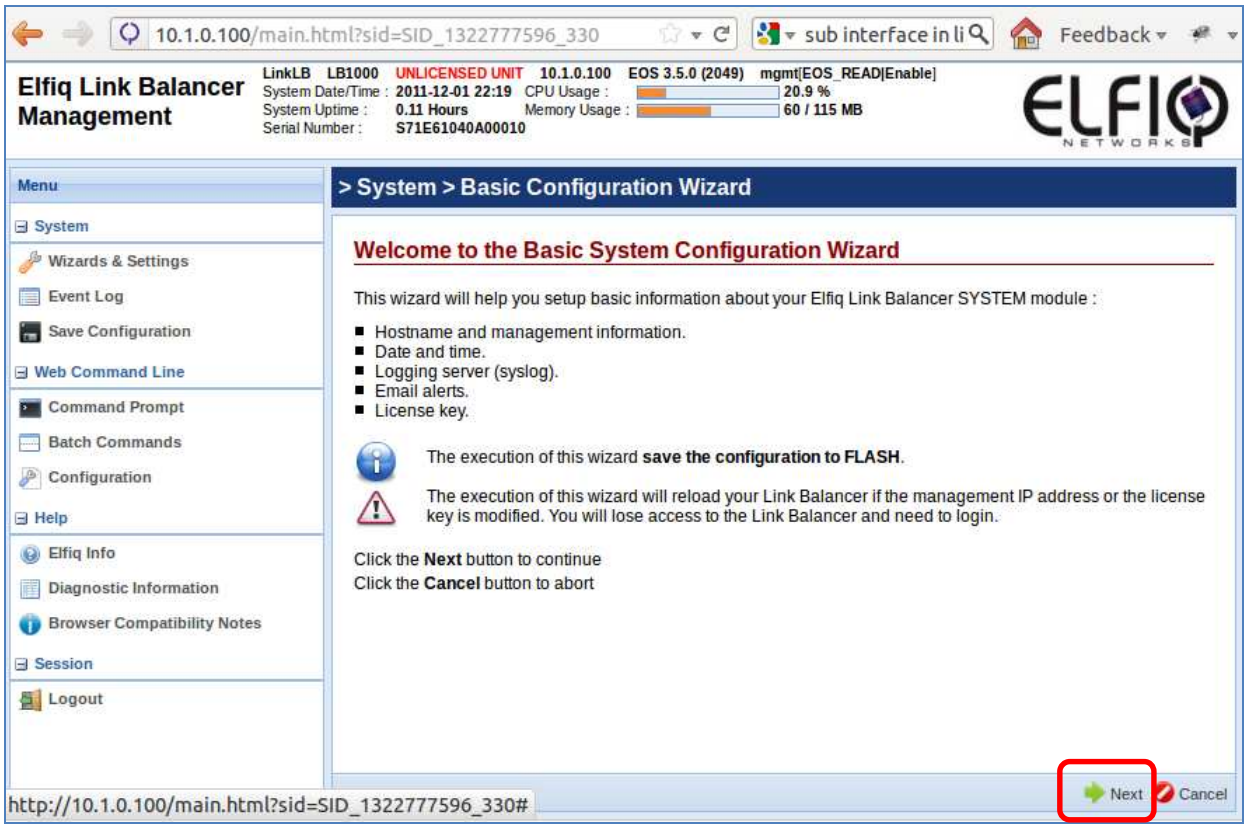
User name "mgmt"

Password "mgmt"

Enable "mgmt"

[4]X can be any digit from 1 to 254 except the 100, and the mask is 255.255.255.0

4. Basic system configuration



Once logged in, a welcome to the Basic system configuration wizard will be displayed automatically[5]. This wizard will help you setup the SYSTEM module of your link balancer. This includes configuring:

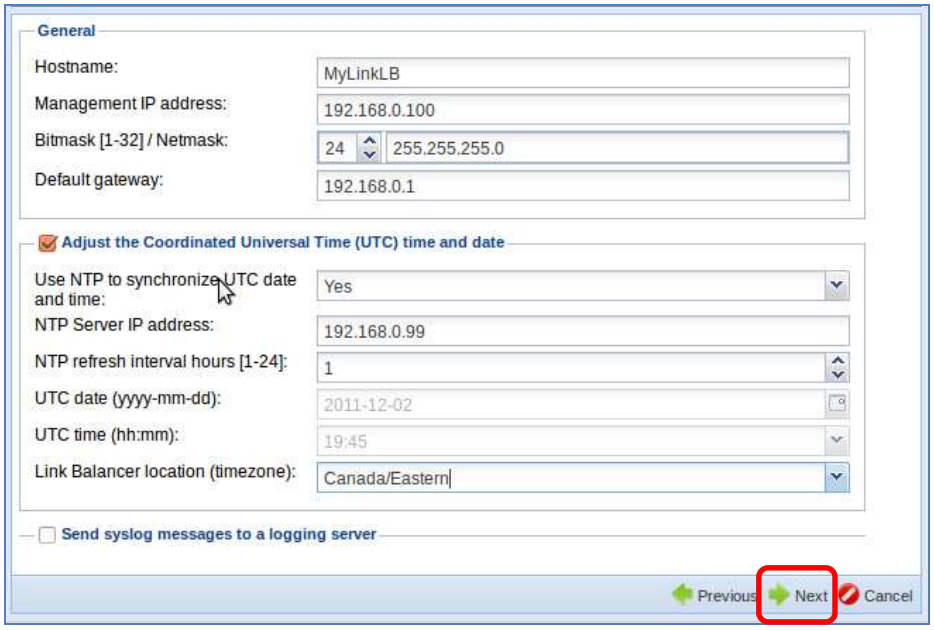
- The Hostname and the management IP address.
- The system time,
- The Logs/alerts, email configuration
- Inserting the License key.

Note that, some preconfigured system informations are also shown on top, most importantly:The model name, the license type, the management IP and EOS version. In our case, the wizard above shows a license type as unlicensed in bold red, this is because we didn't activate it yet[6].

Click **"Next"** to start the configuration

[5]Click on wizards and settings -> basic configuration menu to get to the same wizard
[6]Unless your link balancer unit is shipped to you preconfigured with the license activated, the license type will show as Unlicensed in bold red, otherwise it's in bold blue.

This windows allows you to insert all information

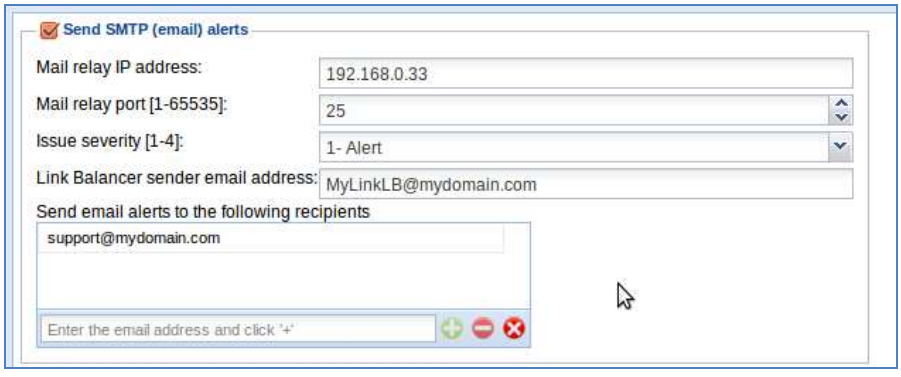


We named the host as MyLinkLB. We assigned to it a management IP address of 192.168.0.100, available on the private network, and a gateway of 192.168.0.1

We configured the date and time on the unit to be synchronized from an NTP server available at 192.168.0.99 with a refresh time of 1 hour. Finally we selected the time zone as Canadian/Eastern. Notice that you can choose not to use NTP and insert UTC time and date manually[7]

We left the box “Send syslog messages to a logging server” unchecked because we assumed we don’t have a syslog in the network.

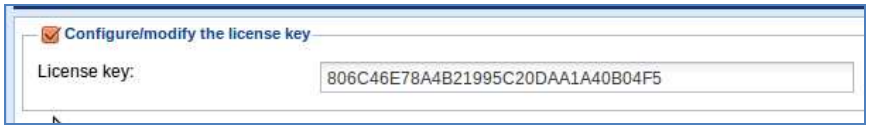
Click **“Next”** to continue.



[7]Please refer to Admin guide for more info.

Here we configured SMTP relay with 192.168.0.33 to receive notification about the status of the unit through email. We put the severity to 1 to receive alerts only.

Finally we give it an email address of mylinkLB@mydomain and added a support@mydomain.com as a recipient for any notification. You can add more recipient if required. Click next to continue



Here we simply inserted the license of 32 caracters long.

Click **"Next"** to continue

Note: The license is emailed to you once you purchased the unit:

Here is an example of an email you should have received

Elfiq Networks Unit Shipment

sales@elfiq.com

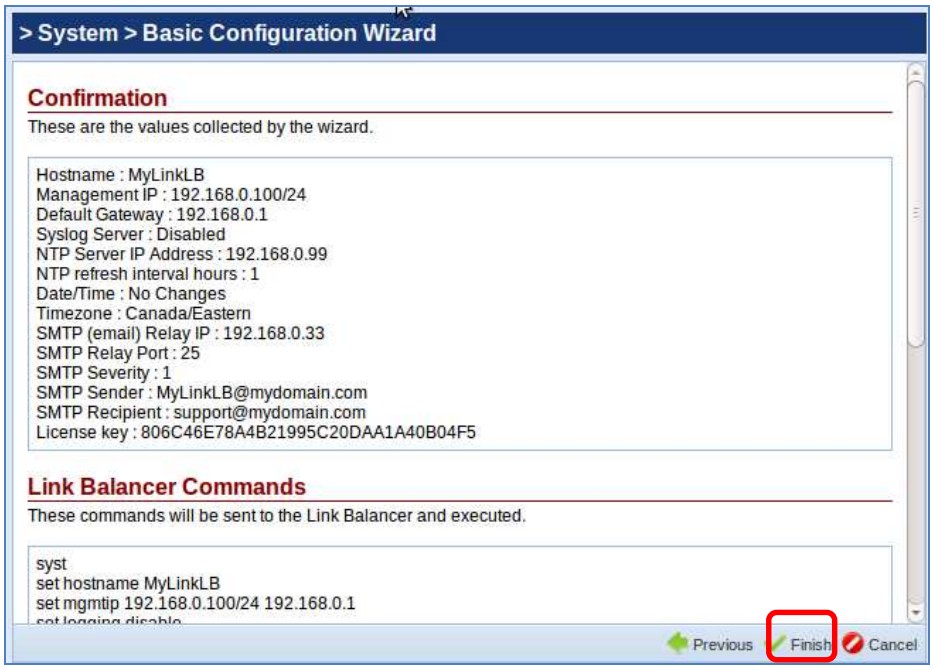
Sent: Wed 31/08/2011 3:28 PM
To: GreatAdmin@GreatCompany.com
Cc: Support; sales@elfiq.com

Message | Elfiq Support 2.3.pdf (349 KB)

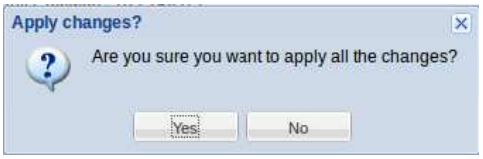
Here is your license key and serial number information:

Unit Owner :	**Great Company Inc.**
Installation Site :	**Great City Office**
Hardware Serial Number :	**12345678**
License Type :	**End User**
License Key :	**18ZVP45Q8BKBLD062WI6H2147S257B72**
Model :	**Link LB-800E**
HA/Failover Option :	**No**
Geographical Option :	**n/a**
Maintenance :	**Partner L3 10/1/2011 to 9/30/2012**

Finally, the wizard will show the summary of what was inserted through the wizard and ask for your confirmation before applying the configuration. If the information shown corresponds to what you intended, just click on Finish to apply the new configuration.



A confirmation box will be displayed



Click **"yes"** if you are sure.

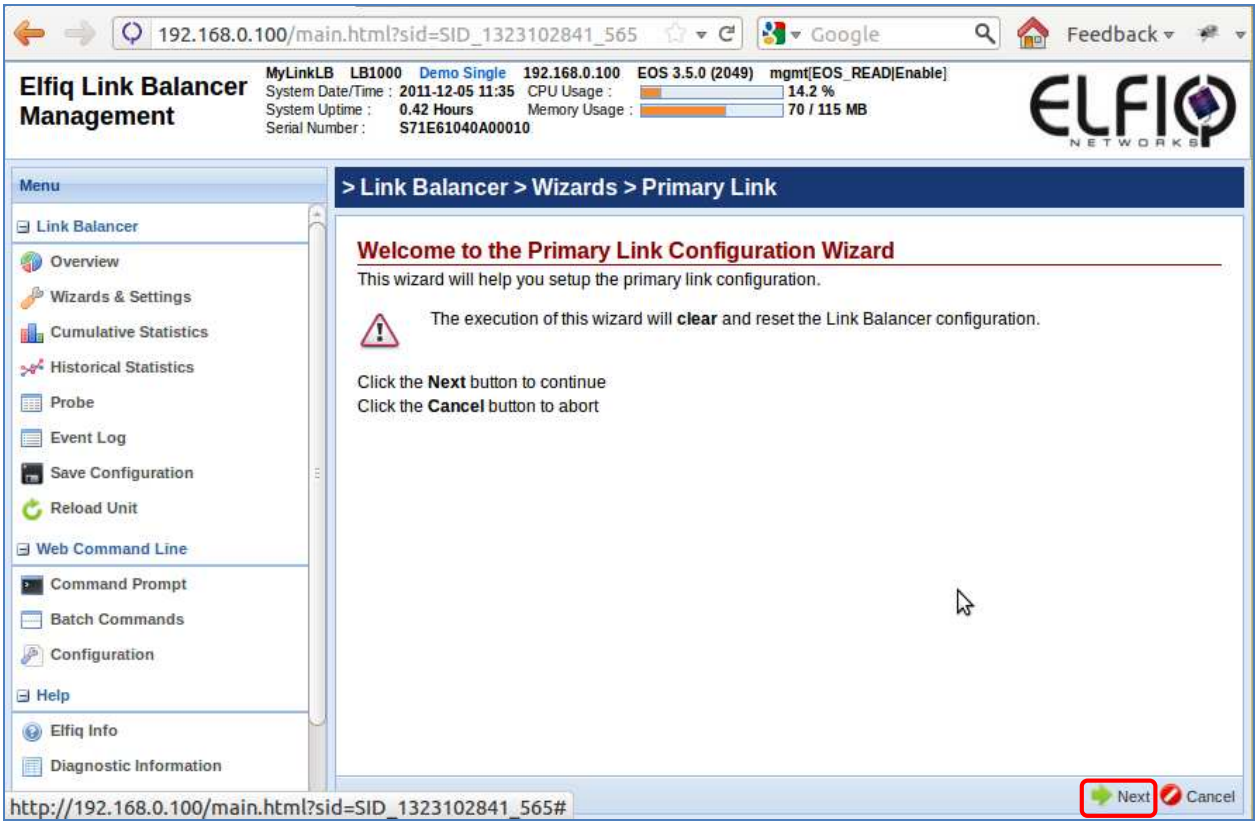
The unit will reboot to apply the changes.

Another box message will be displayed to show that you lost the connection to the unit. Just ignore it and reconnect using the new management IP address: 192.168.0.100

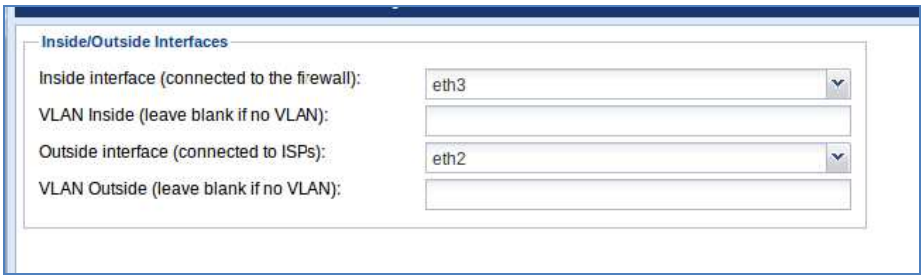
5. Basic Virtual Forwarder Interface (VFI) configuration

5.1. Configuring the primary link

After reconnecting with the new IP address, you are automatically redirected to primary link page to create a new primary link.[8]



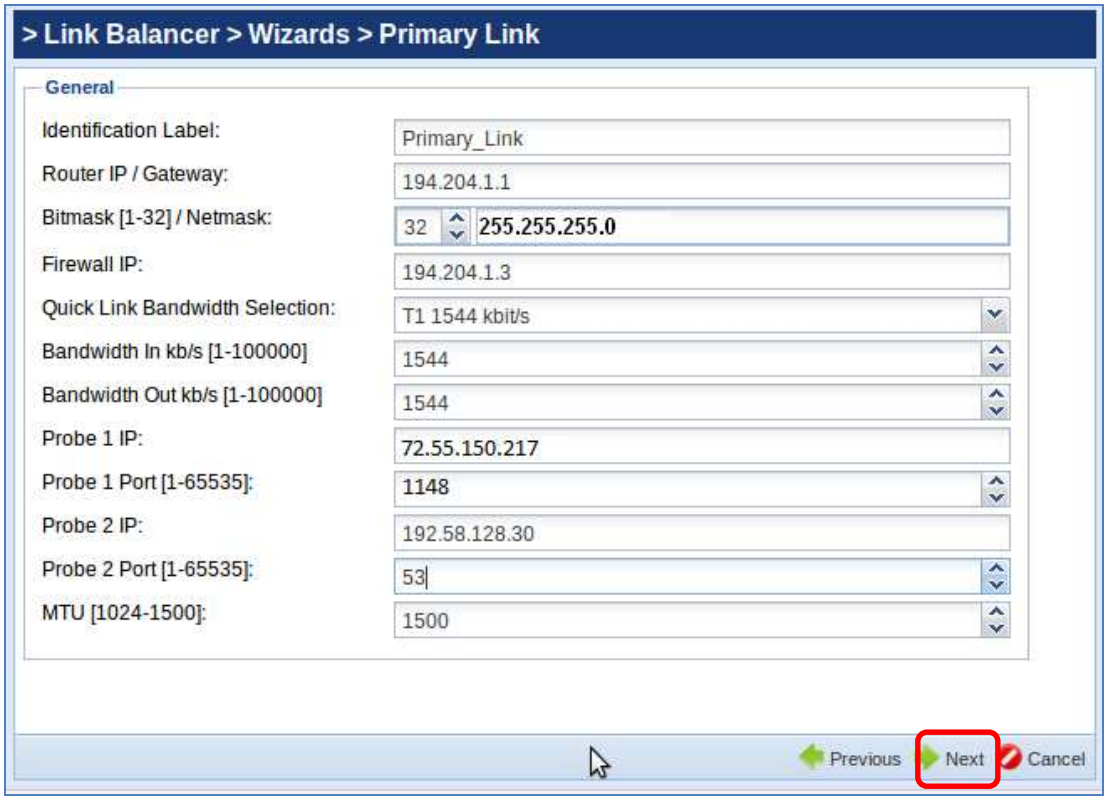
Click **"Next"**to continue



[8] You can get to the same screen through Wizards & settings ->Primary Link.

Here, notice that the wizard automatically defined eth3 as the inside interface, and eth2 as the outside interface, because these are the default failsafe[9] ports on this model. The primary link is supposed to be plugged in the outside interface eth2 (see section 6 for more details).

Click next to continue

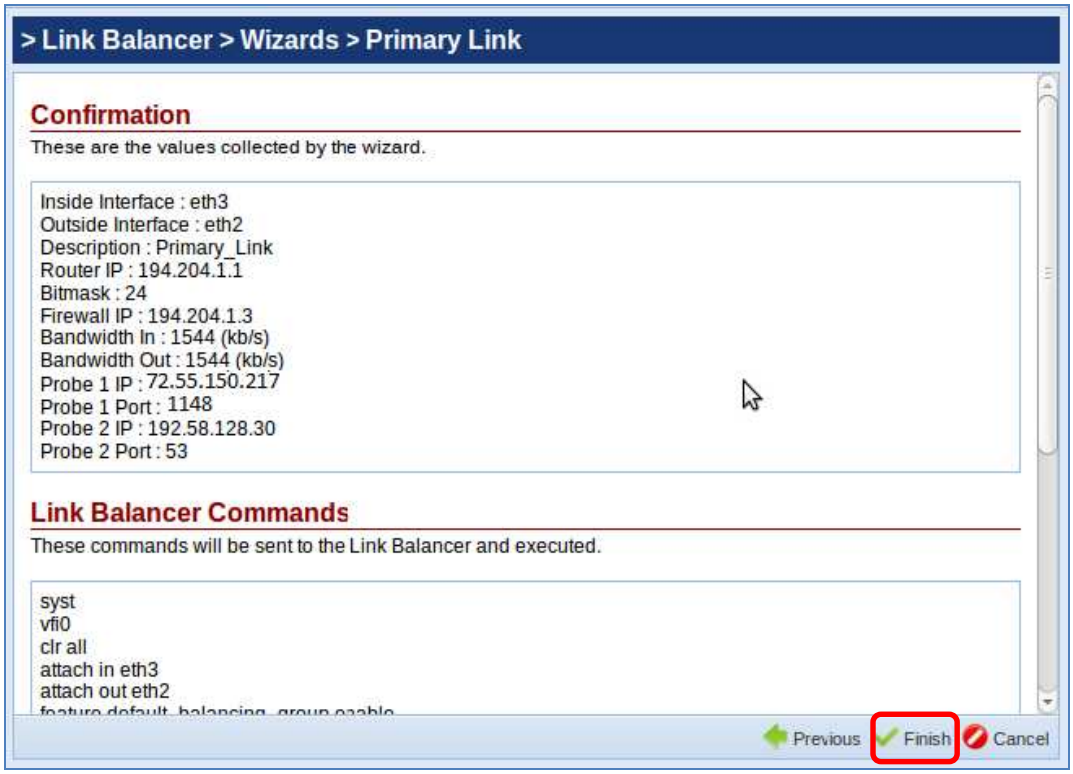


Here is where all primary link information should be inserted. Most of the information is provided by your ISP: IP address of the gateway, the mask, the speed of the connection and also the MTU. The polling destinations or probes however should be defined by you[10]. They are used by the link balancer to check the status of the Link.

Click **"Next"** to continue

[9] Failsafe is useful in order to keep the internet connection through the primary link should the link LB goes down

[10] The probe IP address can be any IP address reachable on the internet that's reliable. Probes could be a root DNS server, a public service or another Elfiq Link LB at port 1148. You should define your own probe destinations.



This screen shows what has been added to verify your information before applying.

If satisfied with the changes, click **"Finish"** to confirm.

A window will pop up confirming the changes have been sent and there were no errors. Click **"OK"**

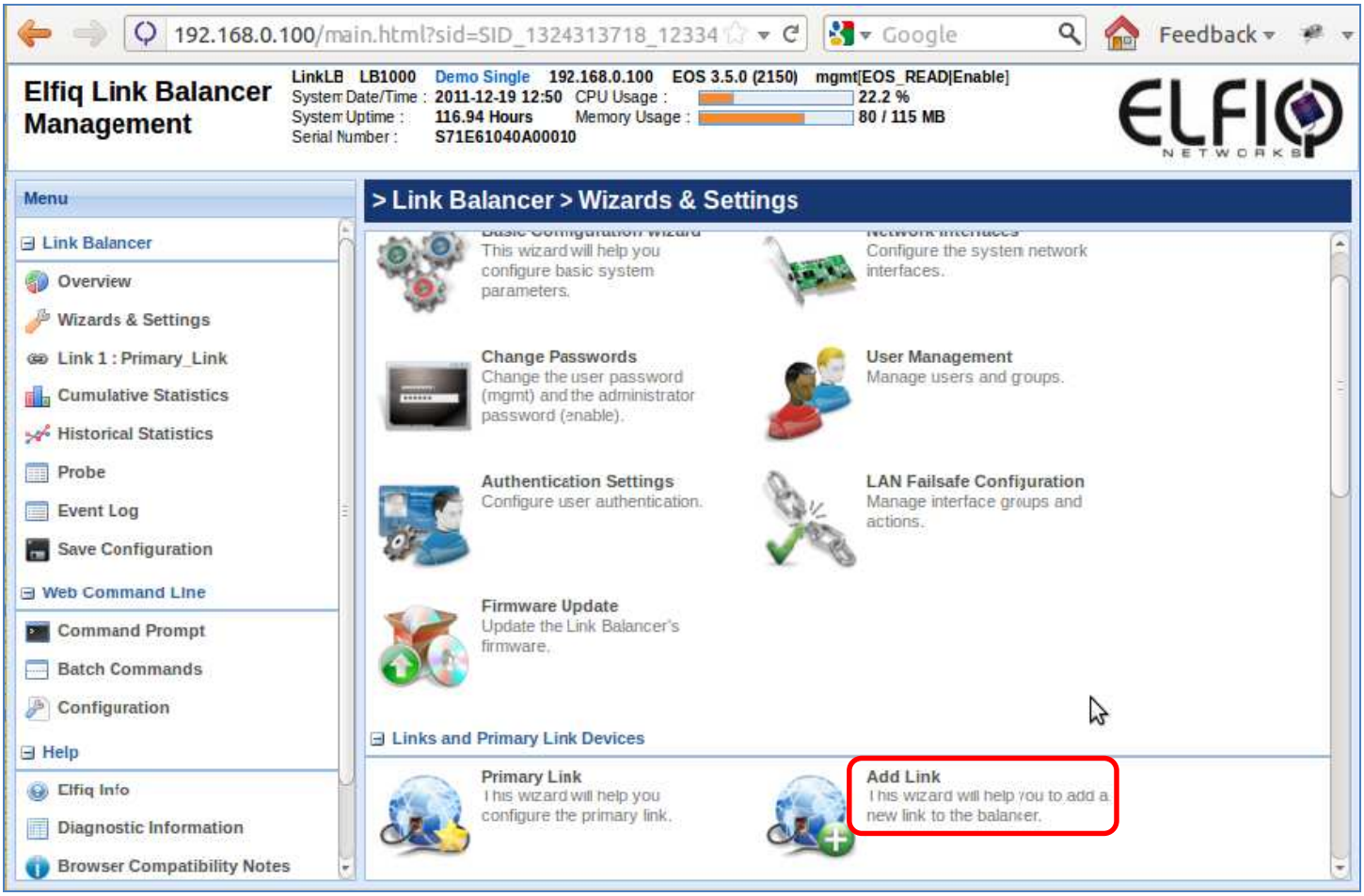
Next we will add an alternate link.

Note: At this point the link balancer can be installed in your network and can operate with just the primary link configuration[11].

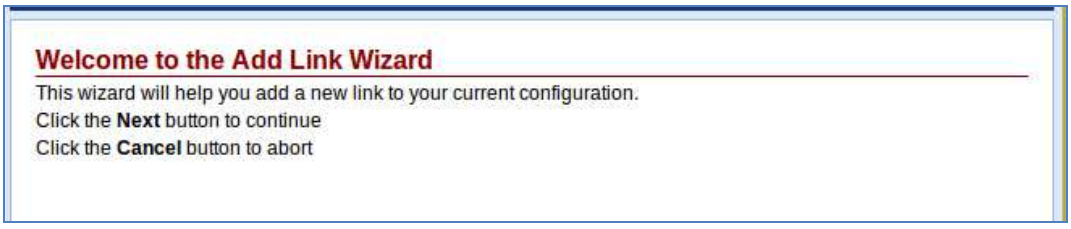
[11] Please refer to section 6**"Installation**" for more details.

5.2. Add Link wizard

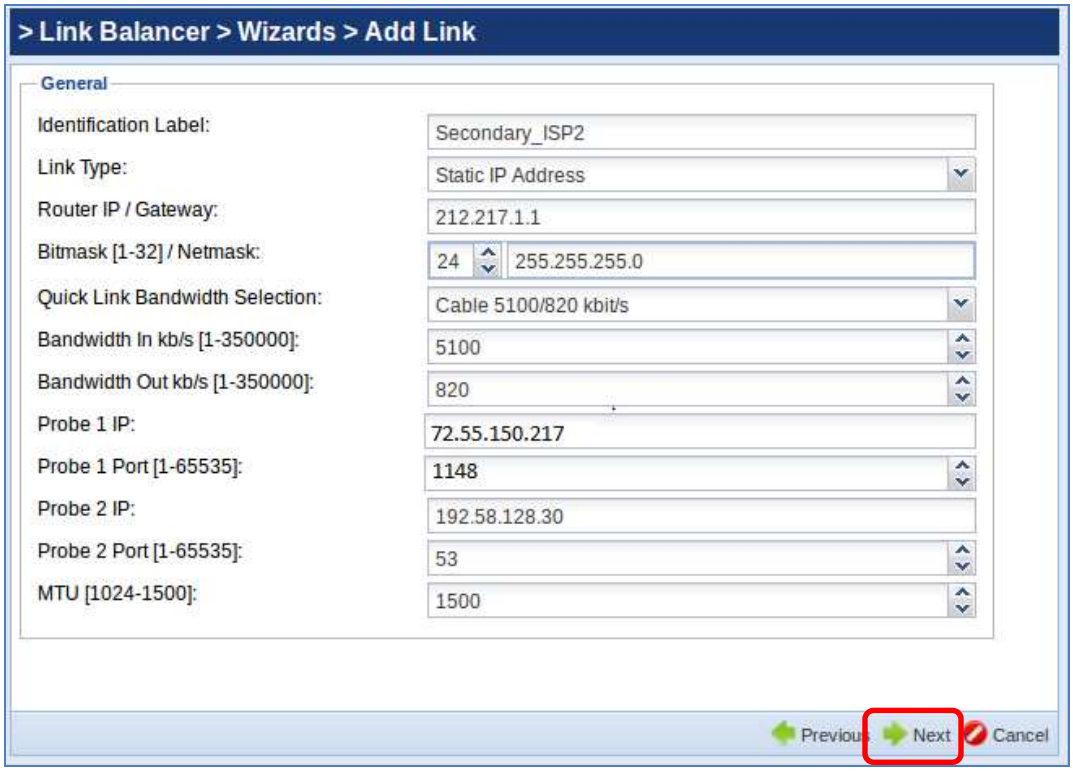
To add an alternate link click on **Wizards & settings ->Add Link.**



A welcome to the add link wizard will be displayed.



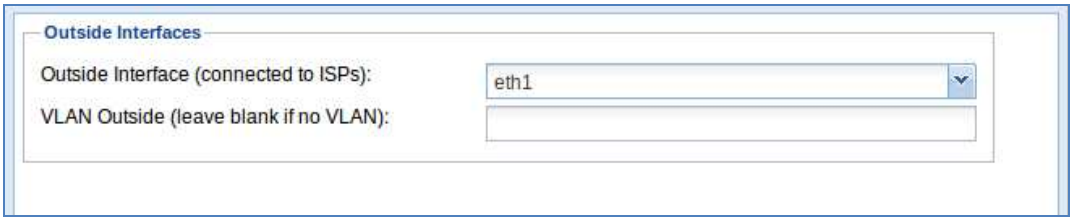
Click **"Next"** on the welcome screen.



In this window, we inserted the IP address of the secondary ISP gateway, the type, the download/upload bandwidth and the probes[12].

Note that the "Quick link Bandwidth" Selection allows you to quickly select a bandwidth from some usual configuration. In this scenario, we selected the Cable 5100/820 Kbits because it matchs our download and upload bandwidth. The Cable in the description doesn't necessarily represent a Cable link.

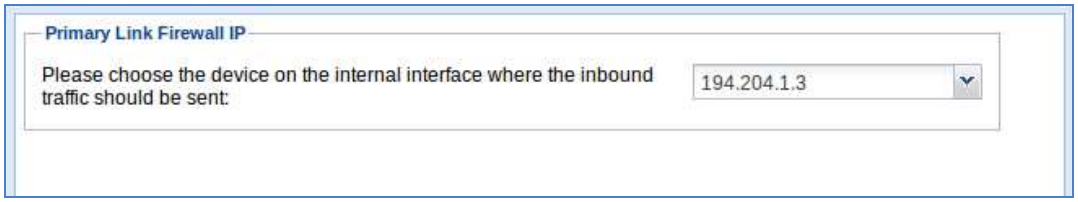
Click **"Next"** to continue.



Here we selected which interface we wanted to use to connect the secondary link (we used eth1).

Click **"Next"** to continue.

[12] The probe IP address can be any IP address reachable on the internet that's reliable.Probes could be a root DNS server, a public service or another Elfiq Link LB at port 1148. You should define your own probe destinations.



Here we defined the primary link IP address to where the incoming traffic should be forwarded. Usually, this is your firewall IP address.

Click **"Next"** to continue.

This is the confirmation page. It shows a description of all the changes as well as the generated Link LB commands.

Click **"Finish"** if you agree with the changes.

You will be prompted

Press **"yes"** to continue.

If successful, a success window will be displayed:

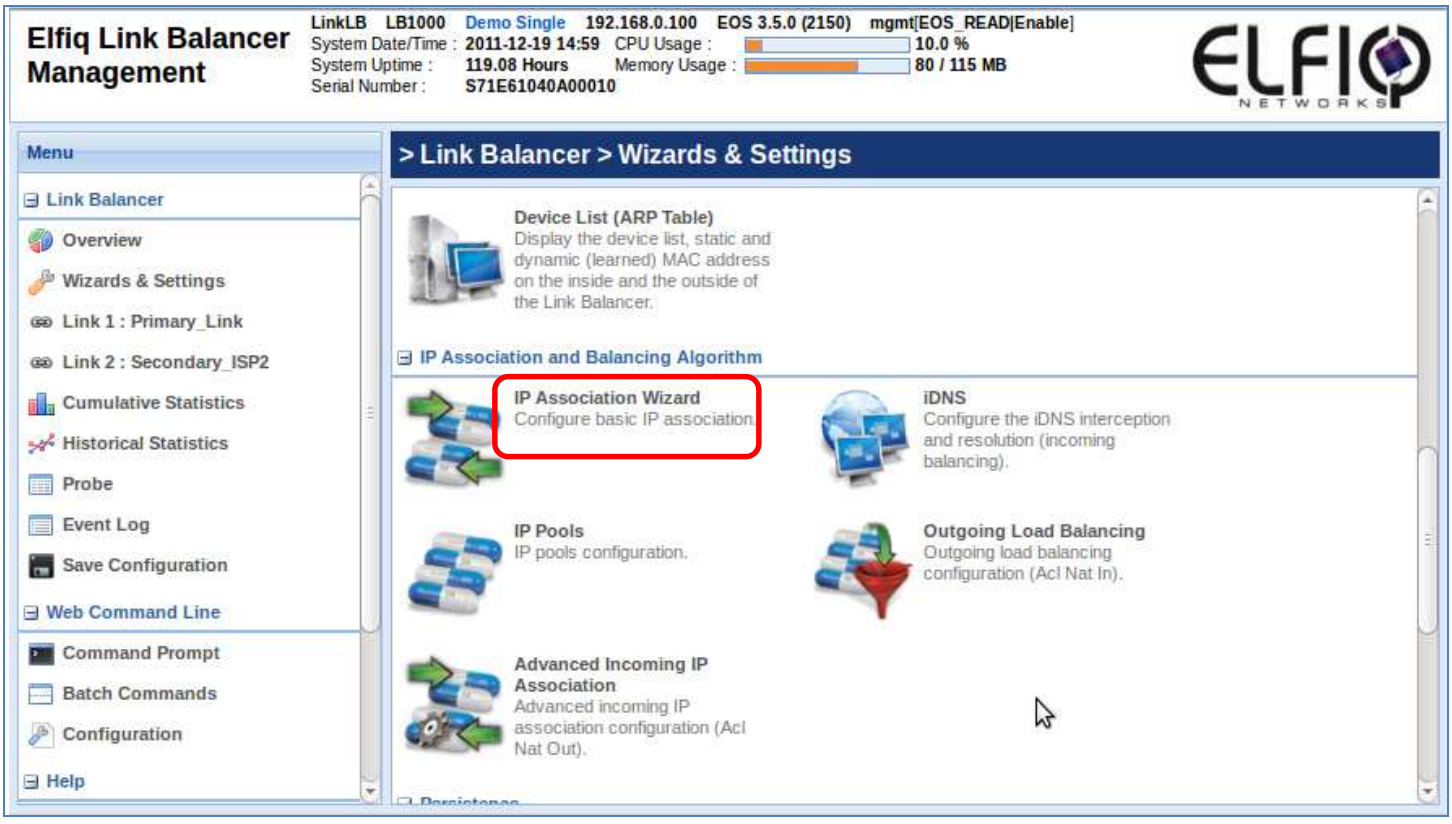
Click **"ok"**.

5.3. Load balancing configuration

5.3.1. IP association

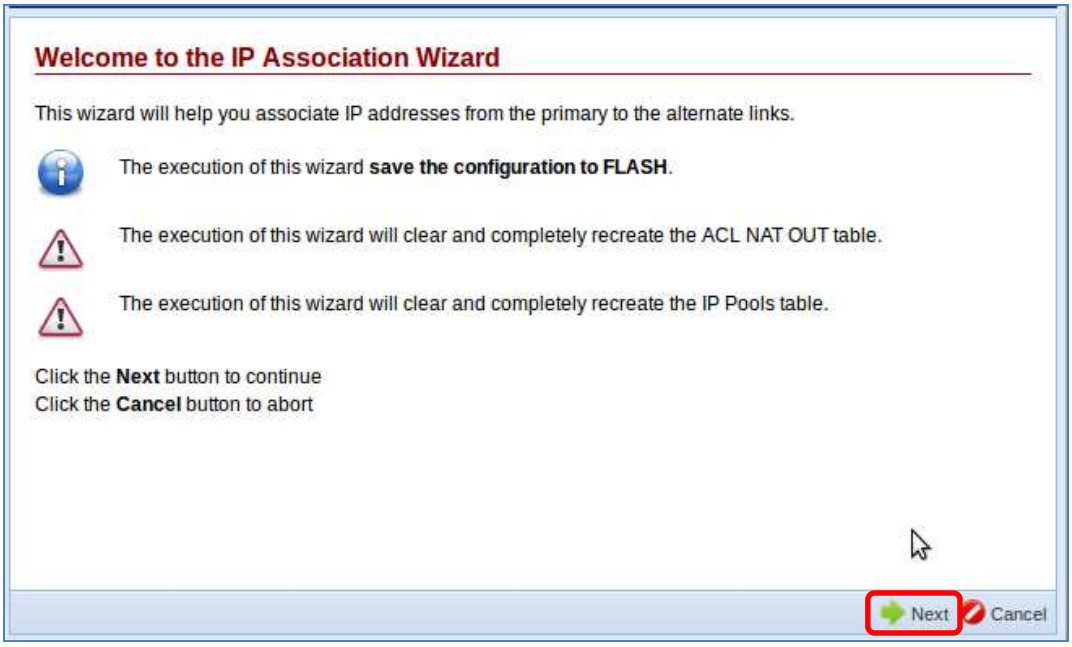
In this section, we will start by creating an association between the "class C" ranges from each link. Creating a basic IP rule covering the complete secondary link IP range is recommended for typical internet deployments as it eases future load balancing.

The IP association wizard will help you match the IP addresses from the alternate links with the IP addresses on the primary link.

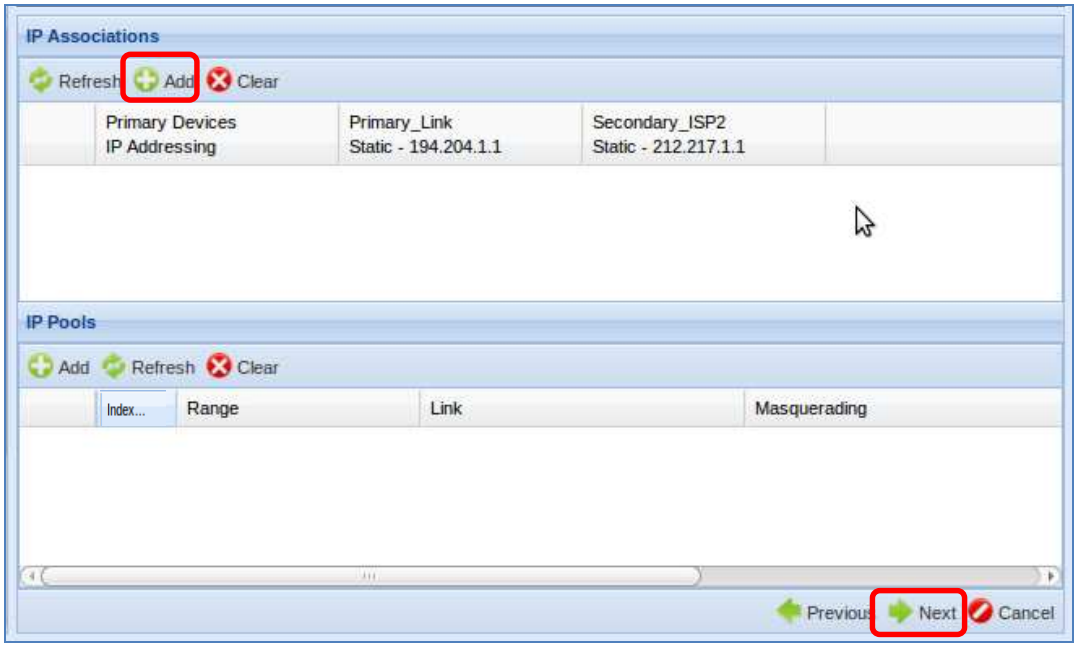


Click on "IP **Association Wizard "**

A welcome page will be displayed.

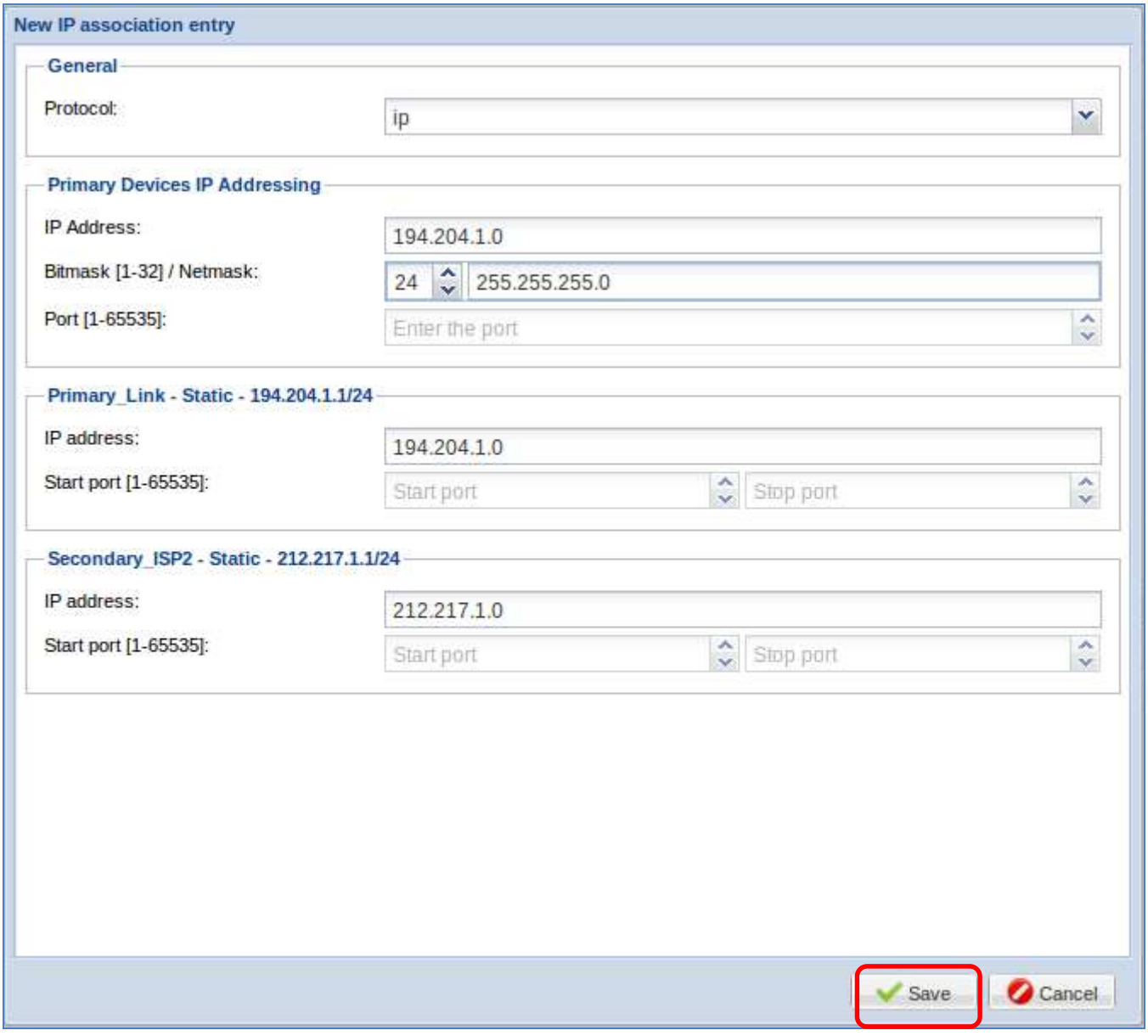


Click **"Next"** to continue.



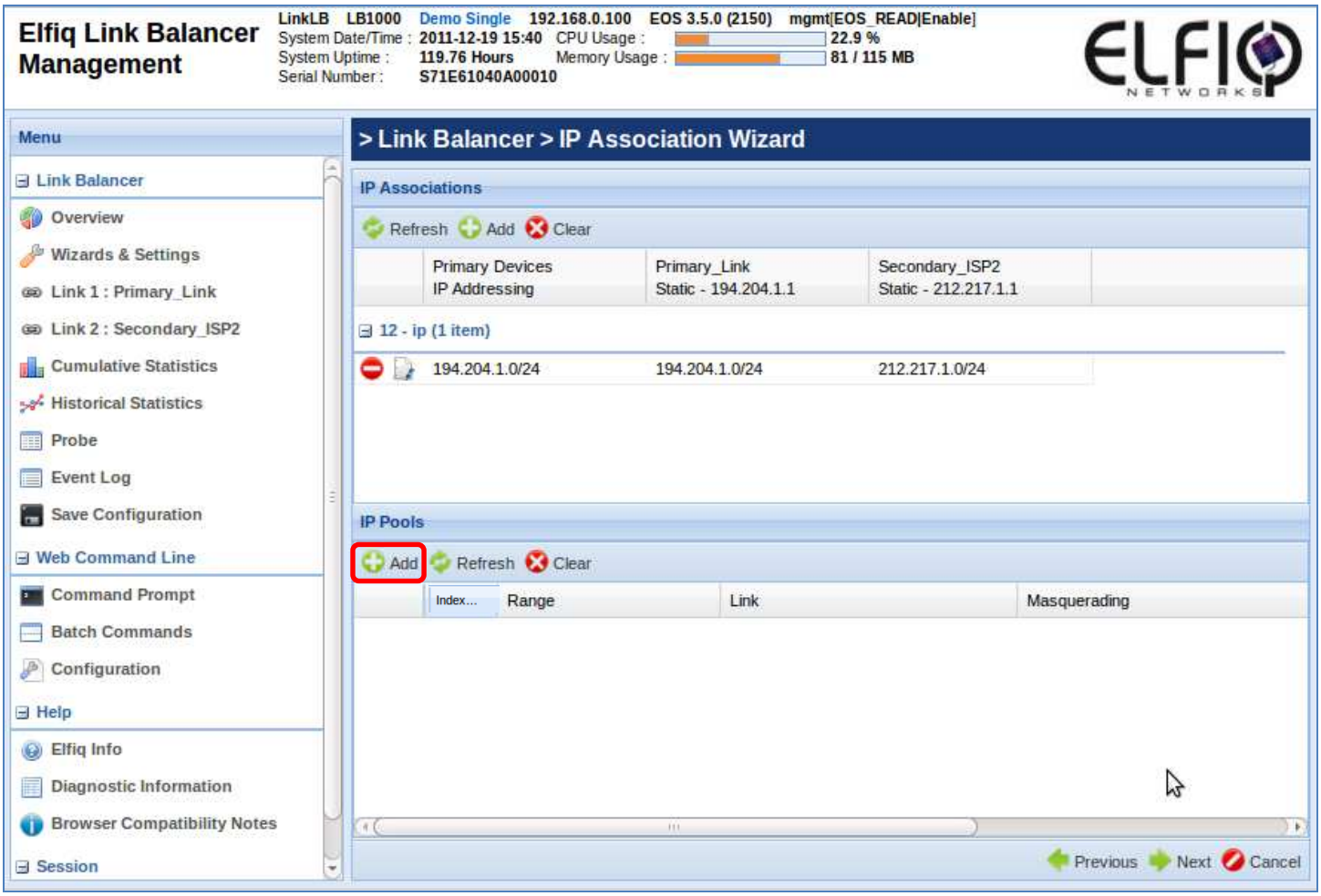
Click on **"Add"** to introduce a new association rule.

The simple IP rule outlined here will create an association between the 194.204.1.0/24 of the primary range with 212.217.1.0/24 of the secondary.



Click **"Save"** when done.

The IP association of the address 194.204.1.0/24 on the primary with the address 212.217.1.0/24 on the alternate link, created is shown in the IP association wizard window below.



After creating your IP associations you should create some IP Pools to use in future outgoing load balancing rules. IP pools help simplify load balancing rules and their updates by using an id instead of an IP address. Plan ahead and create an IP Pool containing the range of IP addresses for each alternate link.

Note: If Alternate link has less IP addresses than the primary Link, we recommend that you create an IP pool containing a single IP (/32) for each link using IP masquerading[13]. This IP pool will be used for load balancing outbound web browsing and similar traffic for all source IP addresses.

To create a new IP Pool click on add under IP Pools

[13] Masquerading maps an IP address to a network address – see the Admin guide for more details.

The new IP pool window will be displayed to insert the related information.

Here we create one pool IP 212.217.1.3/32 to map with194.204.1.3/32 (see section 5.3.2 below). Click Save when done

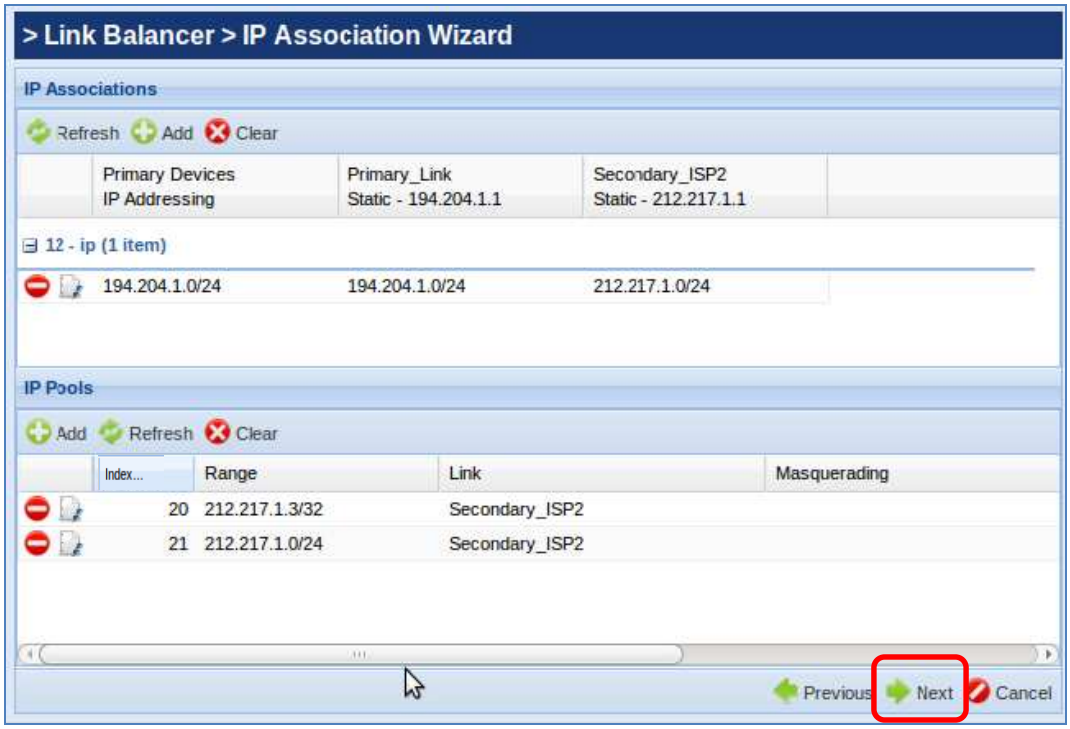
Note: The DHCP id and PPPOX id refer to IP pools for a DHCP and a PPPOE circuits. They are grayed out because in this scenario, we are using static circuits only.

Here, we create another IP pool 212.217.1.0/24 to map with194.204.1.0/24.

Note also that you cannot use masquerading with a network IP address (212.217.1.0). Masquerading is useful if you want to NAT a network to one IP address[14].

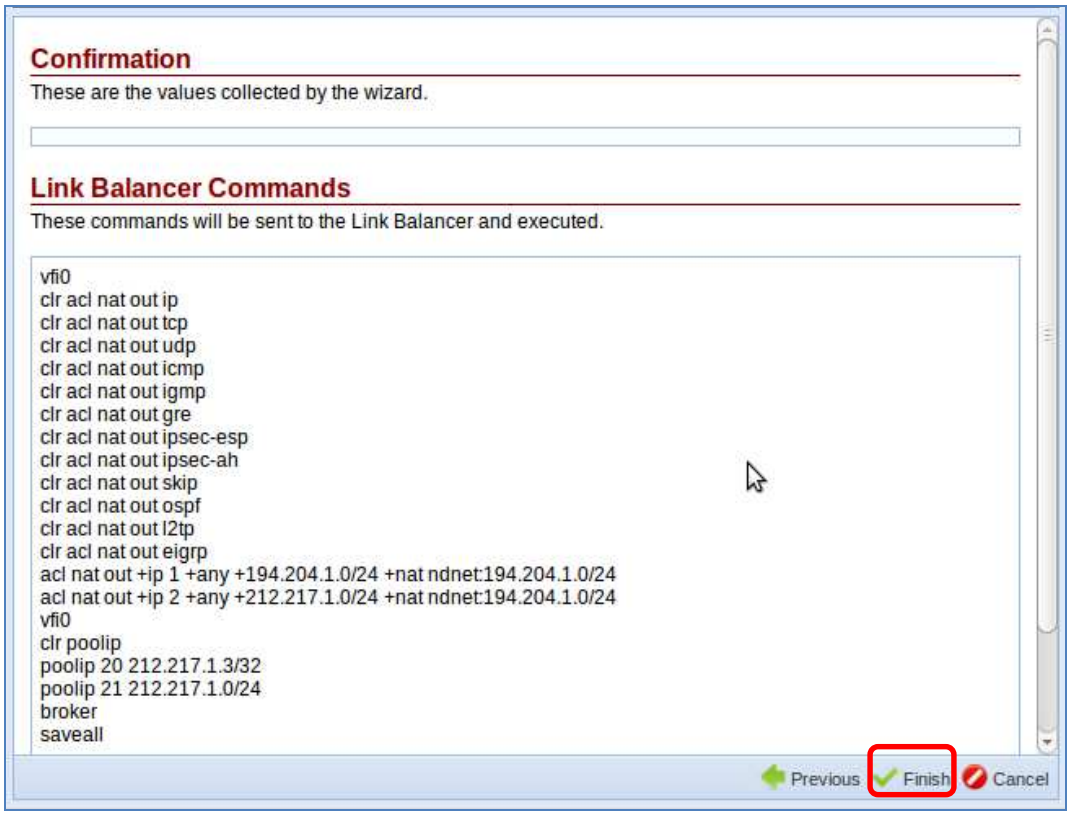
Click **"Save"** when done, the IP pools will be shown on the "IP Associations" window below.

[14] For more information, please refer to the Admin Guide.



Click **"Next"** to continue

A confirmation screen will be displayed with all the related commands that will be applied to the new configuration.



Click **"Finish"** to apply to the configuration.

You will be prompted with

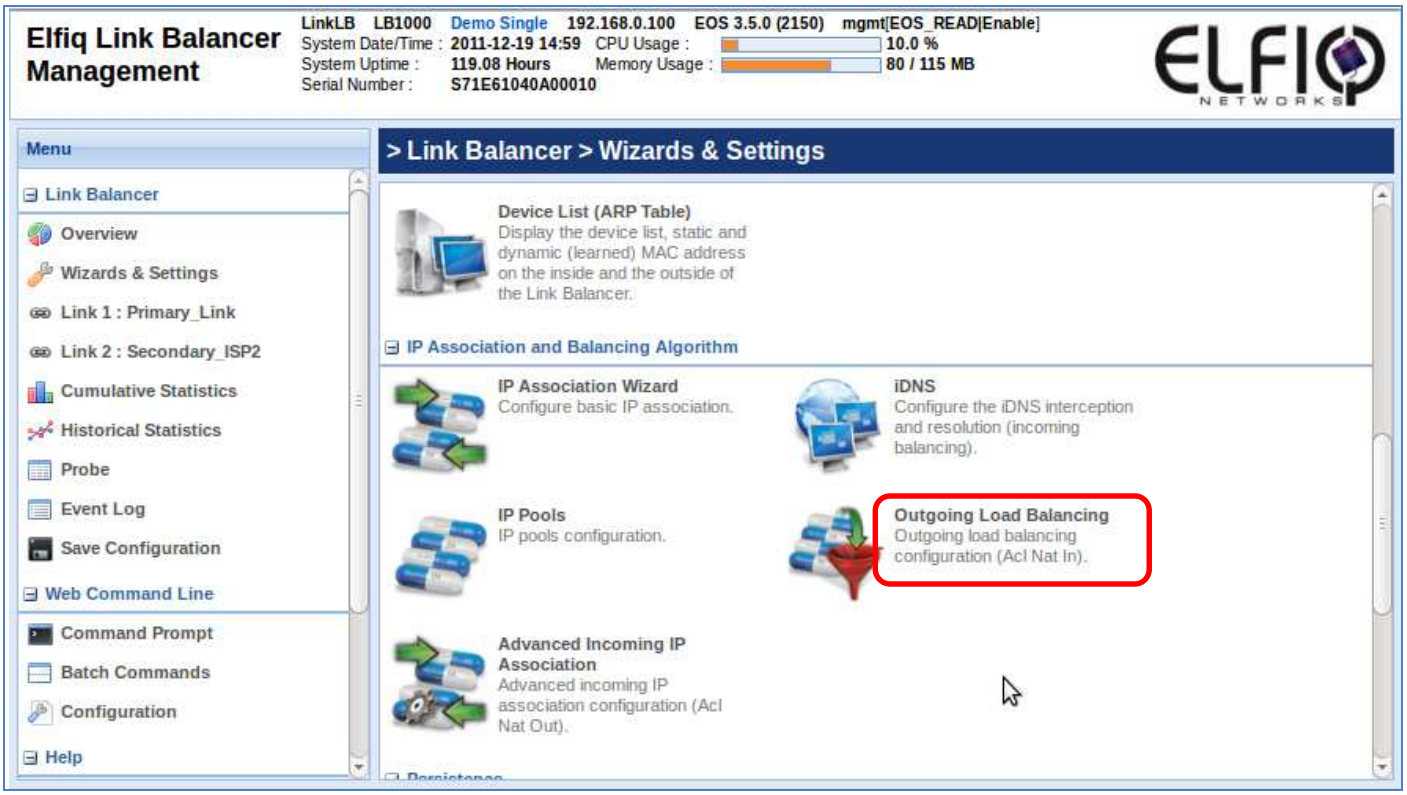
Press **"yes"** to continue.

If successful, a Success window will be displayed:

Click **"OK"**.

5.3.2. Outgoing Load Balancing

Click on **Wizards & Settings -->Outgoing Load Balancing**



This screen allows you to tailor the outgoing load balancing strategies to your network.

Note that the IP pools created in the "IP Association" wizard are listed here for reference. You can also tweak the IP pools here if necessary. Click **"Add"** on top to add a new rule.

We want to create an IP rule. So we selected IP from the protocol list.

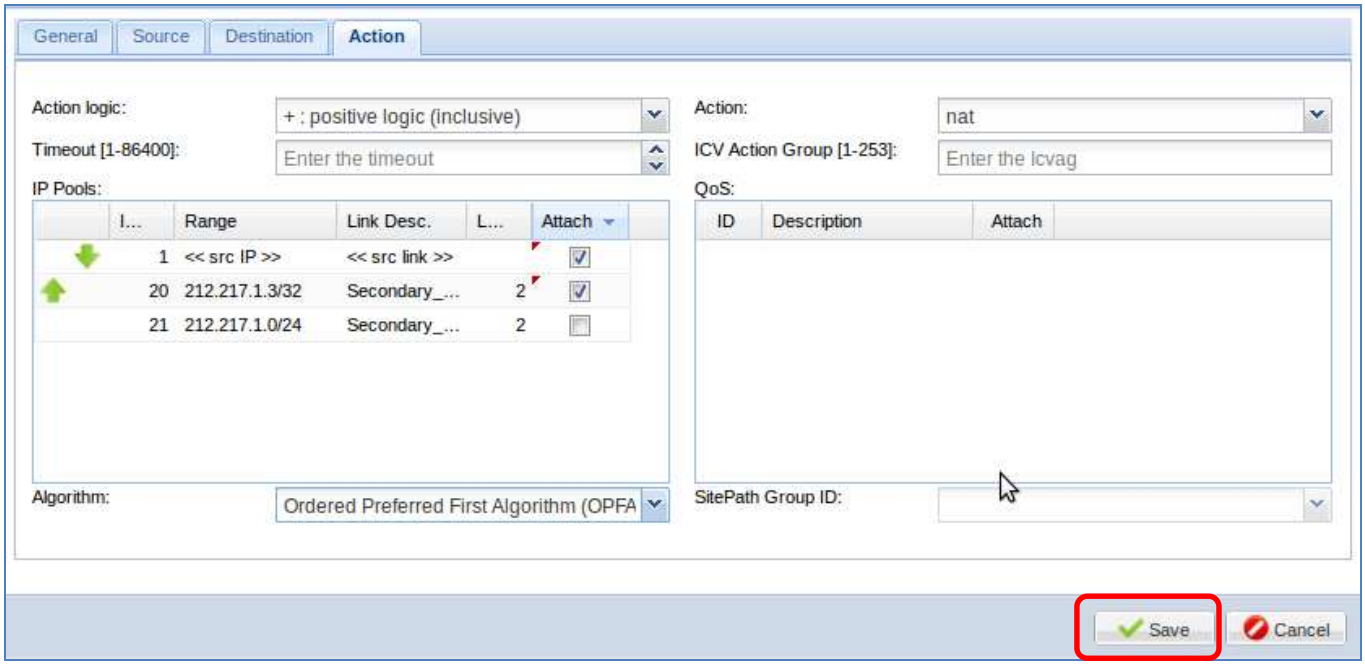
The index represents the order of the rule created. As you see in this example, this is the first rule.

Next clickthe “Source”tab to select the source IP address ofthe rule that will represent the source of the outgoing traffic.

This rule for instance will be applied to any traffic coming from the 194.204.1.3 (the firewall IP address).

Click on “Destination” tab and type in “any” for the destination IP of the rule.

Click on “Action” tab to select the IP pools and the load balancing algorithm you want to use for your load balancing strategy pertaining to this rule.



On the Action logic, positive logic is always preferred. Please refer to the admin guide for more details.

In Action we selected NAT. The Link LB uses the NAT to load balance traffic on alternate links by NATing the source IP to an adequateIP pool of the link in question.

Under IP pools, we checked the boxes in the attach column to select the IP pool 1 and the IP pool 20.

The IP pool 1 represents the source IP that the session will use to get out of the primary link which is basically the same as the original. The IP pool 20 is used when the session is load balanced on the secondary link.

Notice that you can select the order of the IP pool by clicking on the green arrows of each IP pool to push it up or bring it down. The order is important if you are using OPFA[15], but not necessary for other Algorithms.

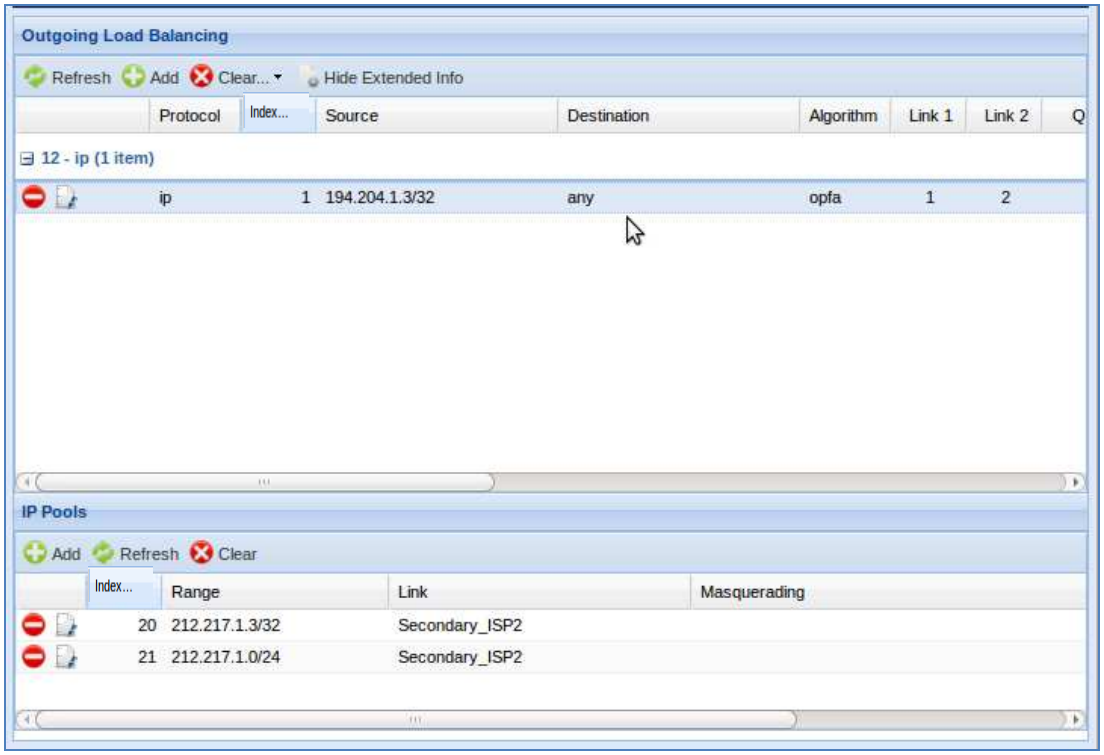
Under Algorithm, we selected OPFA. OPFA is used for a failover[16] strategy. Other algorithms can be selected depending on the strategy you want to apply.

Click on **"Save"** when done.

The new rule is shown on the outgoing load balancing window.

[15] Please refer to the Admin guide for more information on the algorithm description

[16]Failover will NAT the traffic on a secondary link only if the primary goes down.



We will add in the same way, a rule for each server in the DMZ, but before, we will create an IP pool for each:

- An IP pool 212.217.1.100 for the local DNS server ; this will be mapped to the IP address : 194.204.1.100
- An IP pool 212.217.1.101 for the mail server ; this will be mapped to the IP address : 194.204.1.101
- AnIP pool 212.217.1.102 for the web server (http/https) ; this will be mapped to the IP address :194.204.1.102

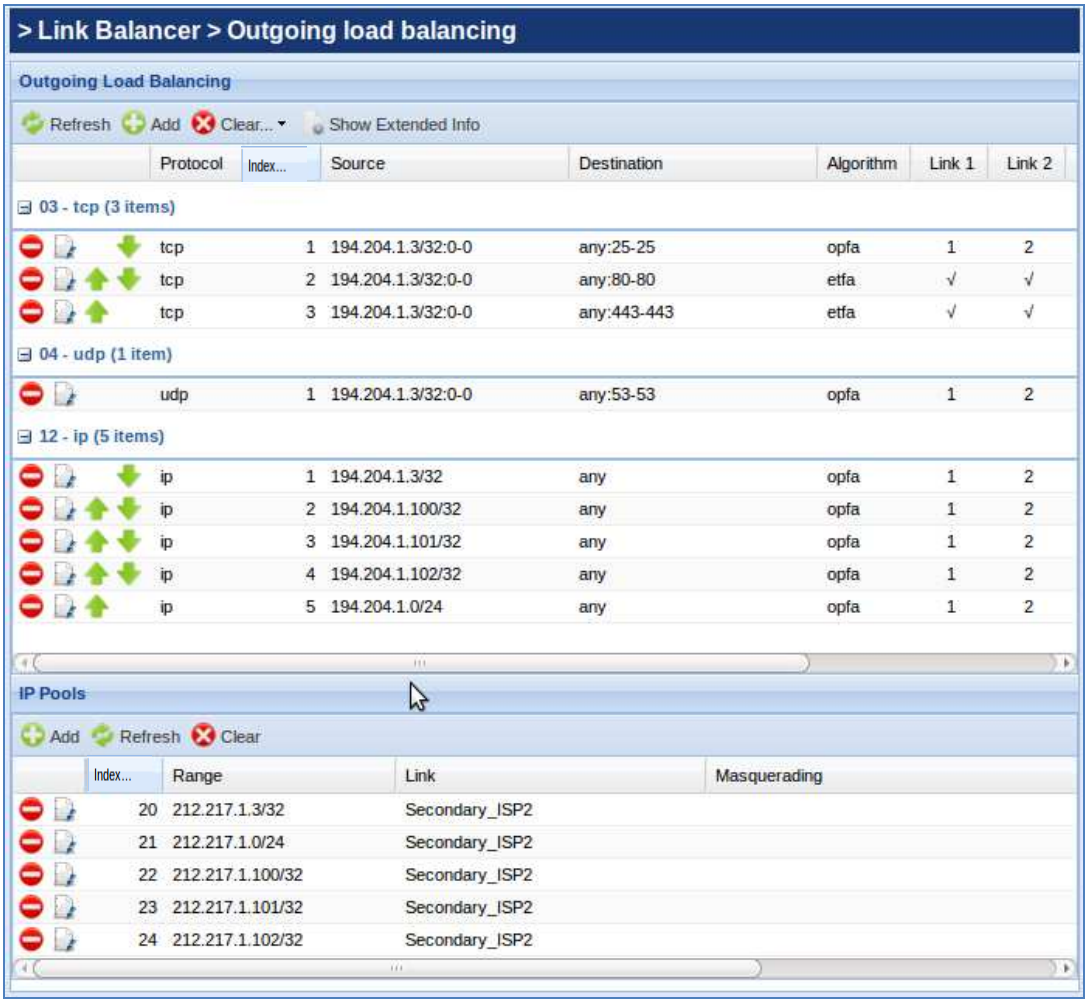
We will create also new rules using the above as a guideline for all protocol types we wish to load balance or failover.

We will start with TCP rules for the ports: 25, 80 and 443. We will define a failover strategy for SMTP and an equalized load balancing for the web and secure web.

We will add a UDP rule for DNS with a failover algorithm.

Finally, we will define a catch all rule for outbound traffic originating from any IP in the Primary Link IP range and using the OPFA Algorithm for a failover.

Once done with the outgoing load balancing strategy, the screen will resemble the following screenshot.



In this example, as it shows in the screenshot, underTCP, threeTCP rules were created. The first rule means all SMTP traffic coming from 194.204.1.3 will go through Link1 first and then Link 2 if Link1 goes down. The second rule means all web traffic coming from the firewall will be equally balanced between the two Links. Similarly, the third rule shows that the secure web browsing is load balanced between the two links and uses again ETFA (Equalized Traffic First Algorithm)[17].

Similarly, a UDP rule for DNS means that any DNS request will go through Link 1 first then Link 2 if the Link 1 goes down.

[17] Please refer to the Admin guide for more details

5.3.3. Incoming Load Balancing

Incoming load balancing allows your clients to get to your network services from the outside, through all the circuits. Should one of the links fail, the client can still get to the network from other links.

Usually, because your resources are originally configured with only one IP address from the primary link, the only way to get to your network from outside is through the primary link only. To overcome this limit, the Link LB knows how to forward traffic to the right server even if a request is coming from an alternate link. It does that by NATing the destination IP address according to the mapping already configured on the unit (as we did above - see IP associations).

The Link LB can also be configured to answer DNS request using iDNS. This way, the requester will only need to know the FQDN[18] to access a resource in your network. The Link LB will answer with an IP address of the resource that can be either an IP from the primary or the alternative link.The advantage of this method is that Elfiq LB will never reply with an IP of a circuit that is failing because, before replying, it checks the status of the circuits and make sure it's up. Furthermore, algorithms can be applied to change the way the link balancer will answer to DNS requests therefore, defining your incoming load balancing strategy.

In order to configure iDNS you would first change your original A records to an NS records for each link on your original DNS server. This NS record will point to an address of an interceptor that is configured on the Link LB.

See Figure 2, for more details: Different steps are described in order to delegate DNS resolution to the Link LB[19].

[18]FQDN : Fully qualified domain name
[19]For more details about IDNS please check the Amin Guide.

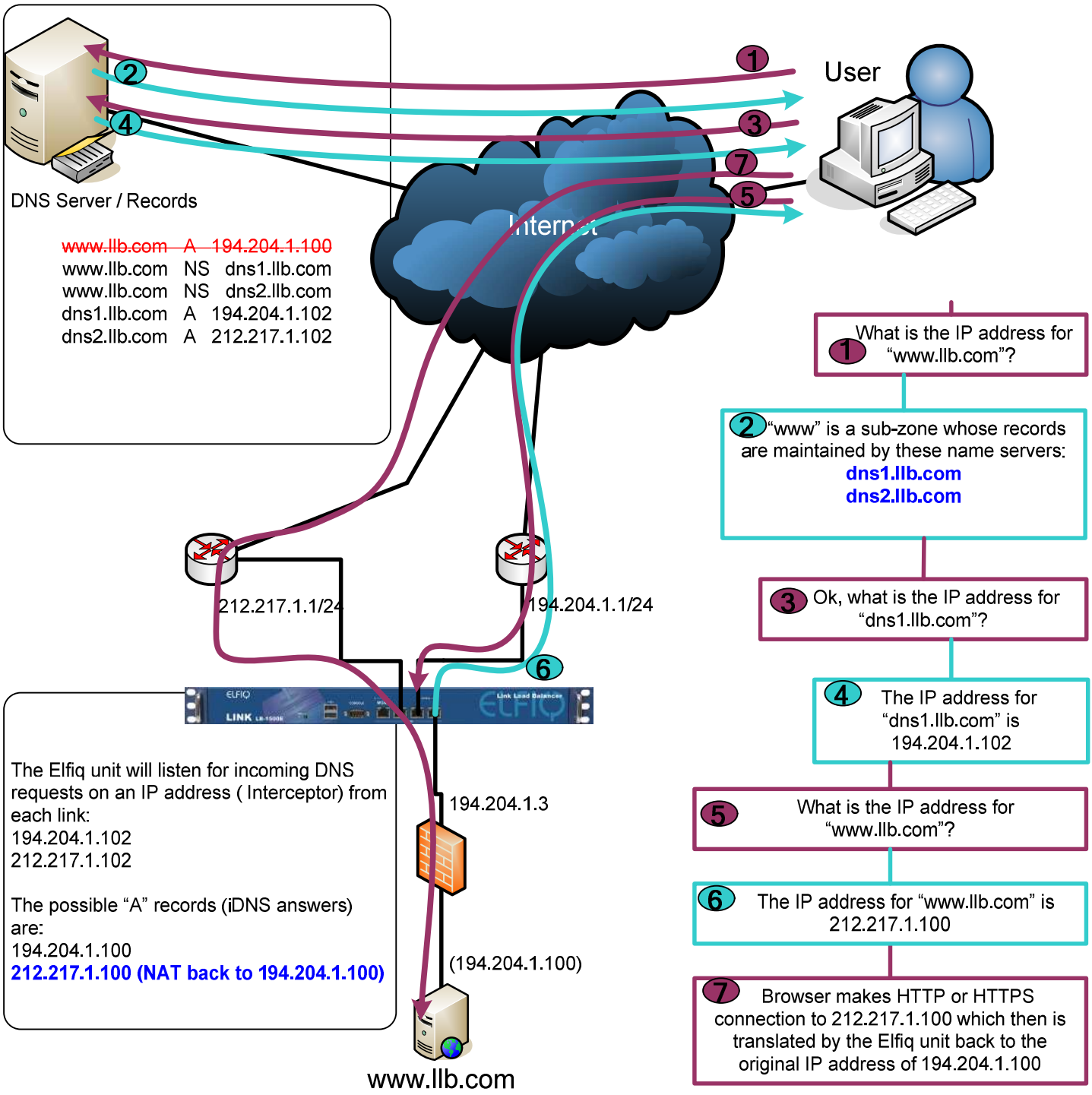
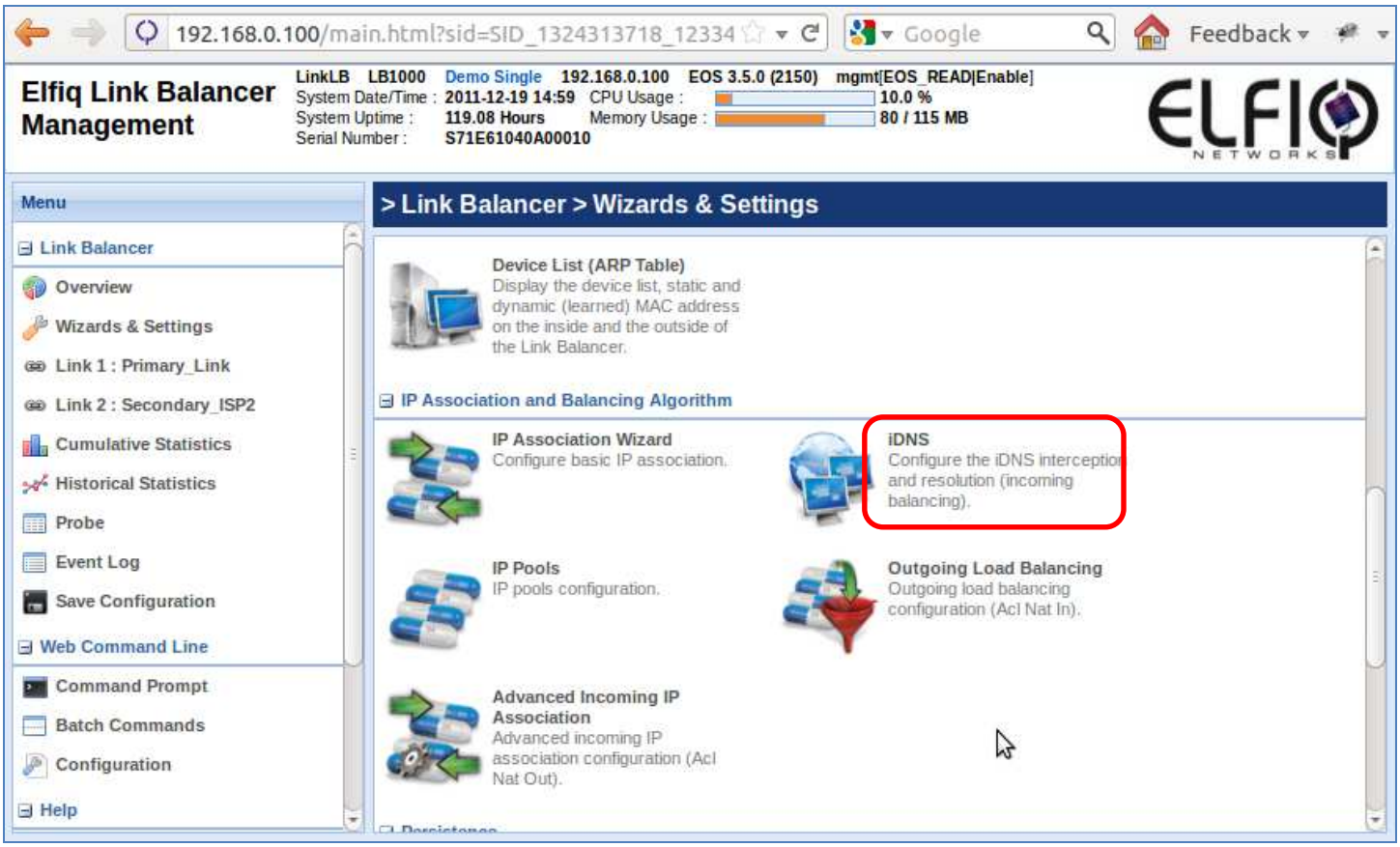


Figure 2

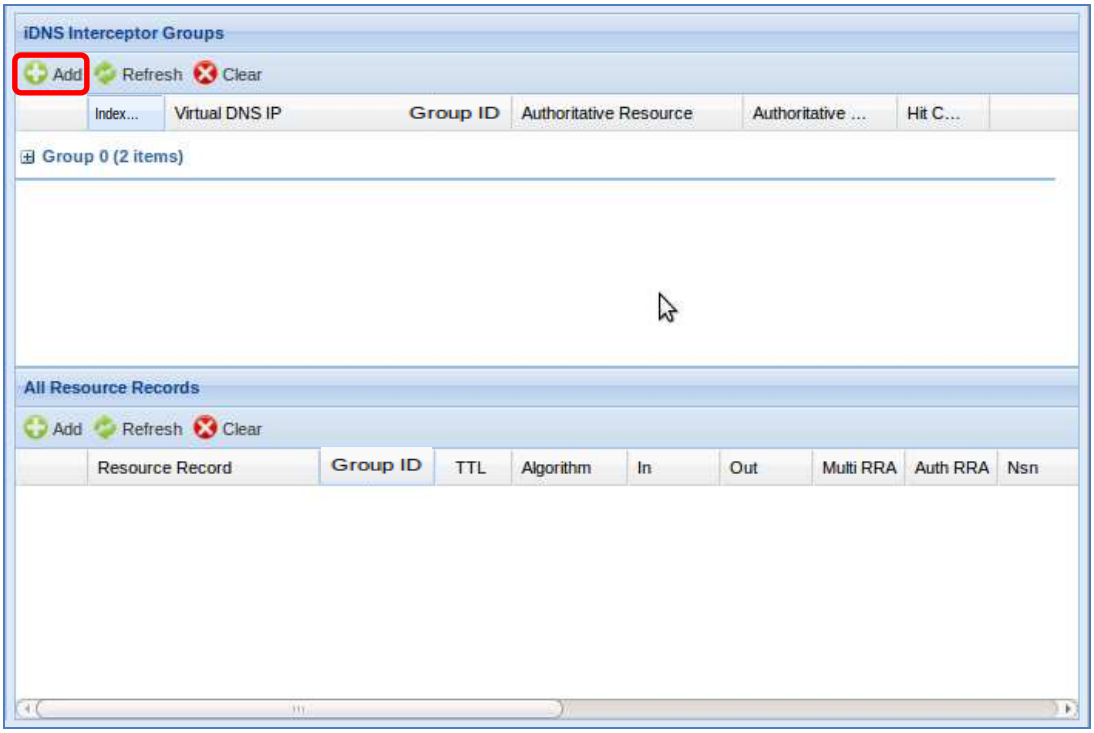
In the Figure 2 above, we replaced the www.llb.com "A record" to an NS record that point to 194.204.1.102 or 212.217.1.102, which are the interceptors configured on the Link LB. At this point, the Link balancer is responsible to answer DNS requests forwww.llb.com. On the Link LB, we configured the A record for www.llb.com to be 194.204.1.100

and 212.217.1.100. Elfiq will answer with an IP address according to the load balancing policy applied(we will define later in this section in associated iDNS resource records).

To configure iDNS on the Link LB, click on **Wizards & Settings --> iDNS**



Click **"Add"** to add a new interceptor



A new window will pop up

The index defines the Id of the interceptor[20].

The Virtual DNS IP address is the interceptor IP address20[20].Usually one interceptor is required per link.

The group ID can be any digit that will represent a group of different iDNS interceptors. Multiple groups can be created to represent different IDNS interceptors groups. As you will see later, we will also need to reference the group when we create the A records[20].

Authoritative resource is a virtual FQDN of the interceptor[20].

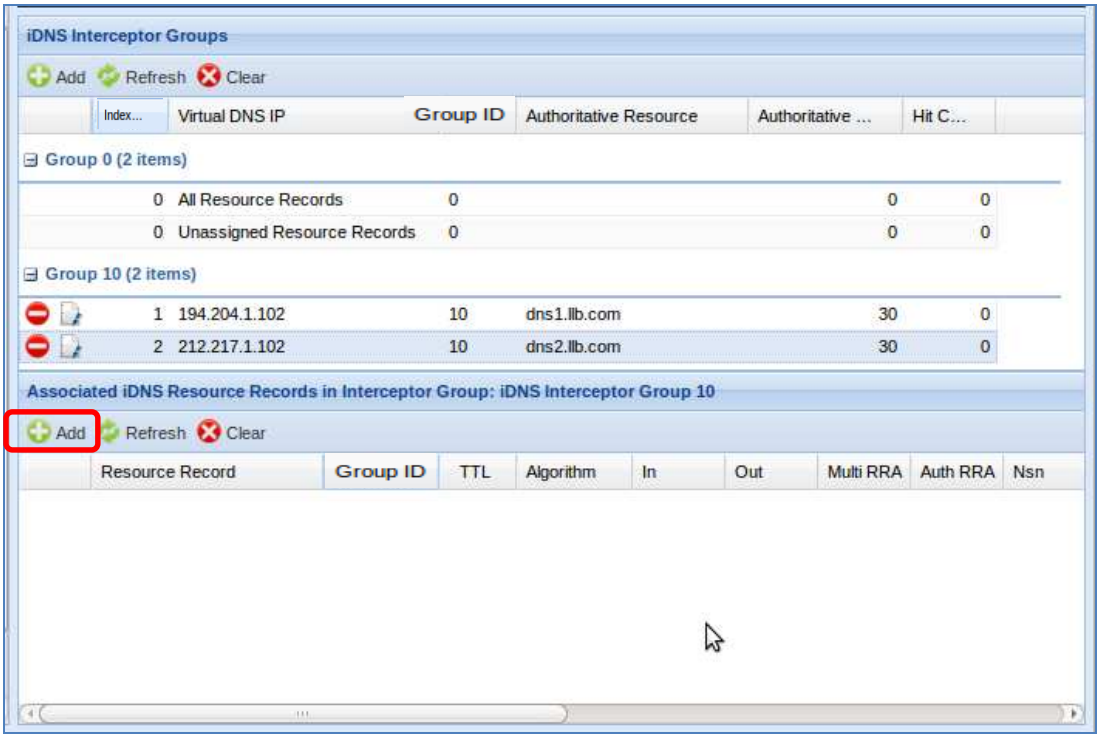
The authoritative TTL (Time To Live) defines the time tocache the entry in the DNS cache[20].

Click **"Save"** when done.

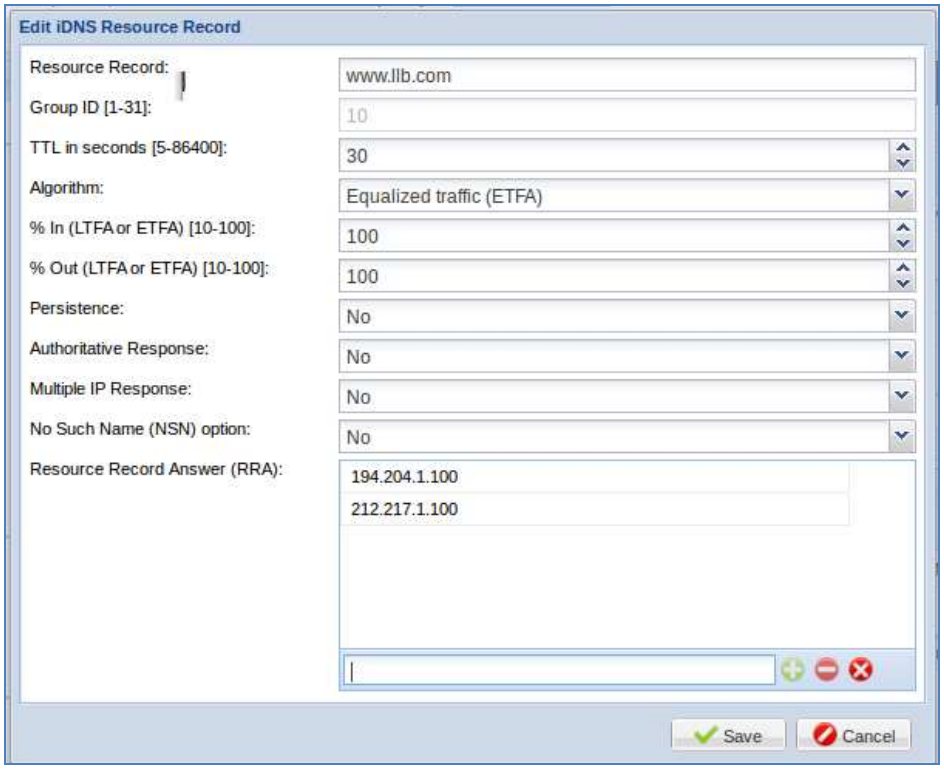
[20] Please check the Admin guide for more details.

Do the same thing to create another interceptor for the second link that belongs to the same group.

This is how it looks after the interceptors are created. And grouped in group 10



Next we will add some resource records. One resource record is required per service to performincoming link balancing. Click **"Add"** under associated iDNS.



The “resource record” defines the FQDN of your resource.

The “group ID” 10 is related to the interceptors we created earlier.

The “TTL in seconds” (Time To Live) defines the time tocache the entry in the DNS cache

The “Algorithm” defines the incoming load balancing strategy[21].

The “In%” and “Out %” define the saturation thresholdsof incoming versus outgoing traffic for this resource. This is applicable only for ETFA and LTFA.[22]

The “Persistence” ensures to keep the incoming sessions on the first link on which they have been initiated. They are identified by their source IP they coming from.

The “Authoritative Response”is “no” to define that the Link LB is not the authoritative DNS server for this resource.It is mandatory to have it at no if your DNS server is externally hosted.

The “Multiple IP Response” option allows the link LB to answer with all possible IP addresses for the service on top of the recommended one by the algorithm.

The “No Such Name”will reply with “no such name”[21].

The “Resource Record Answer (RRA)” defines the IP addresses of the resource in each circuit we want the resource to be accessed from.

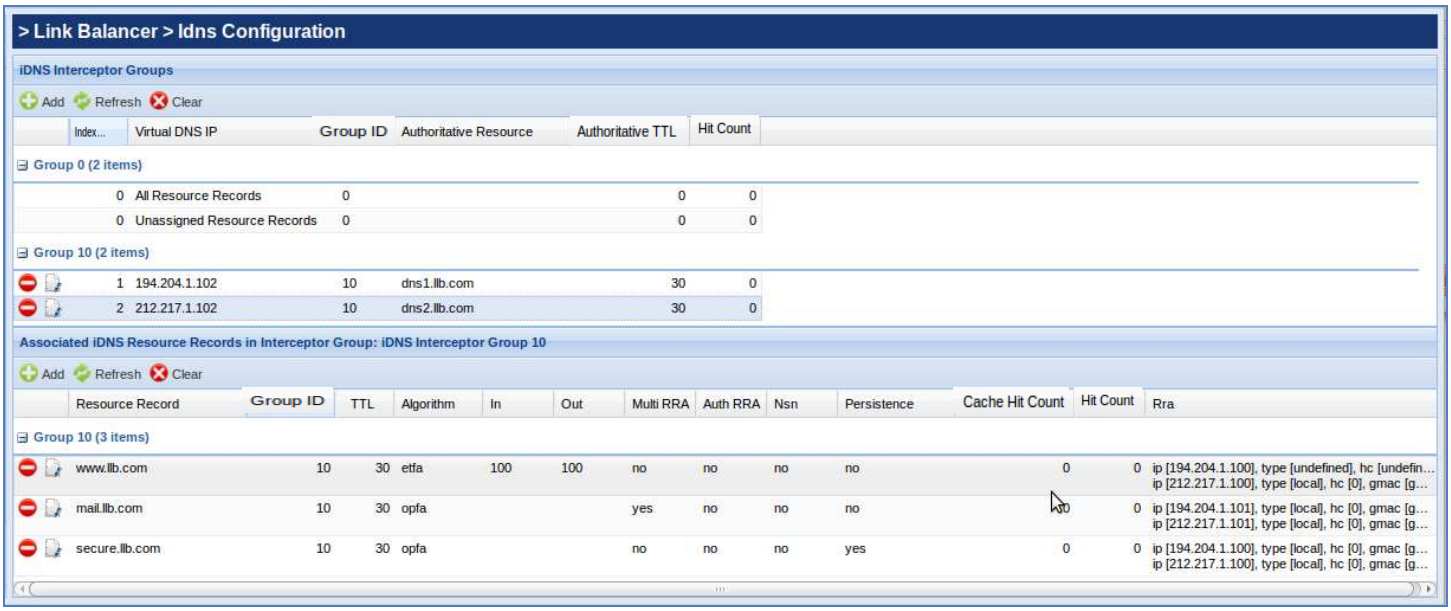
[21]Check the Admin Guide for more details on the Algorithms.
[22] Note that these are not the threshold of the links, defined in section 4.1 and 4.2

Following the same principles, other resource records will be added.

A mail.llb.com is added for the mail server.

A secure.llb.com is added for the secure web server.

This is how itwill look like when all resource records are added.



Notice thatall resource records are related to the group id 10 of the interceptors created earlier.

We also selected “Yes” for multi RRA to answer with multiple IP addresses for any DNS request regarding the mail server. For the secure web server we used persistence to keep the session on the same link for the period of a session (see under the persistence column).

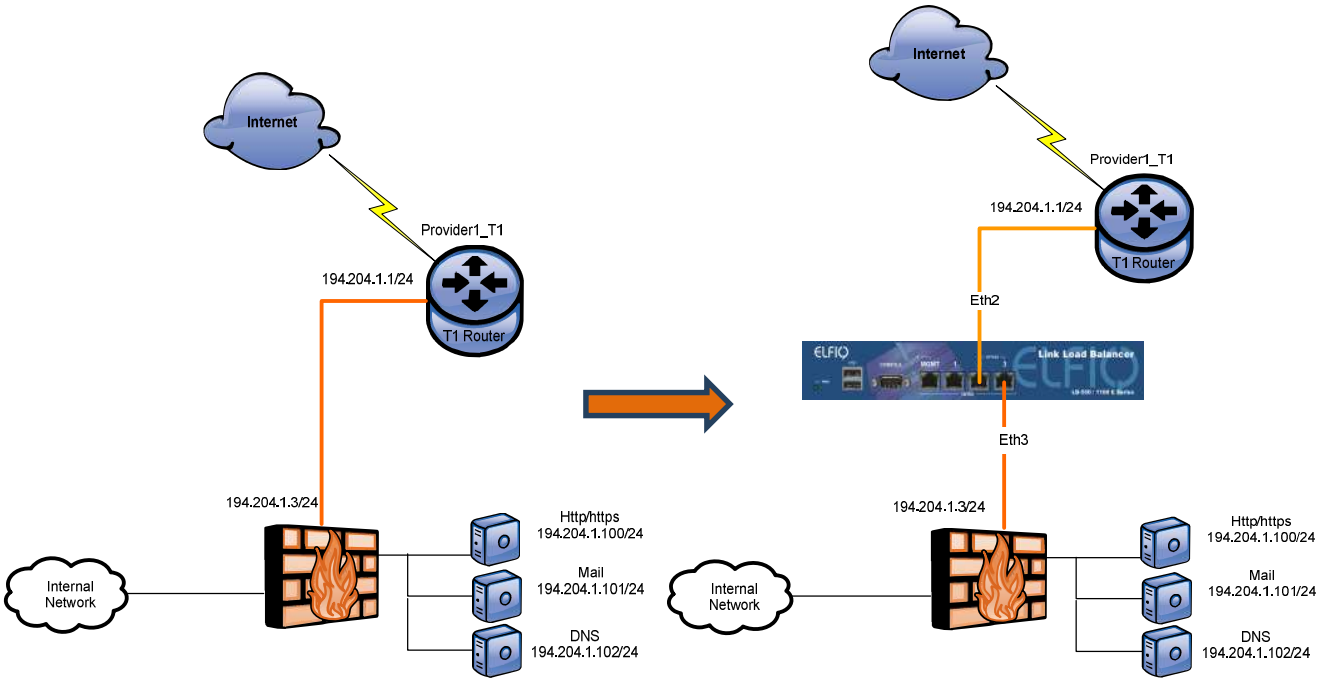
Note also that all the records are created with one IP address from each link. Should one link fail the link balancer will answer any DNS request with an IP address of the link that’s available and thus the client can always get toyour services through the available links.

6. Installation

This step requires you to temporarily disconnect your firewall from your existing link router in order to introduce the Elfiq unit.

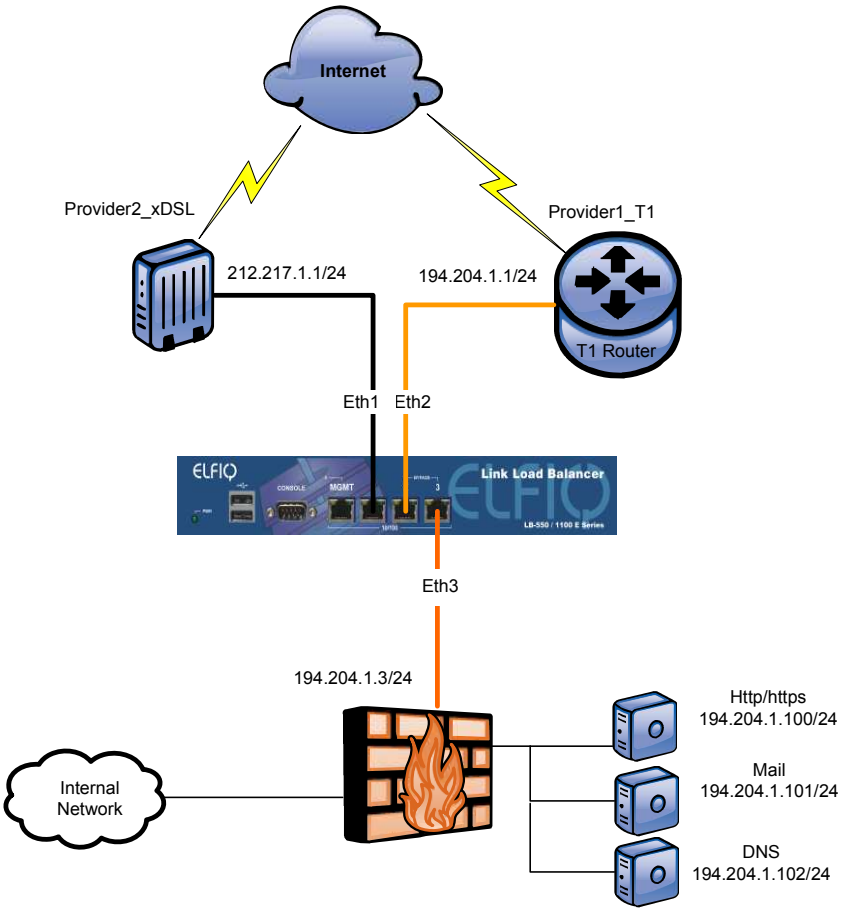
In this example we will use an Elfiq LB550E. In this model, the port numbers in the failsafe[23] mode are port Eth3 and port Eth2 (Port numbers may be different for your model). Connect your firewall on the inside interface Eth3 and the primary link router on interface Eth2. (Please use a crossover network cable unless you are connecting the Elfiq Link LB to a switch). All traffic will start going through the Elfiq Link LB

NOTE: Before you turn on the Link LB, check your Internet connection, it should be working. If no connection is established, check your cables.



Once you are sure you have connection to the internet, connect the interface Eth1 to the secondary link DSL modem and turn on the unit.

[23]Make sure you always use the ports in failsafe mode to connect your primary link and your firewall. This mode will keep the connection between your firewall and the primary link up should the unit fail or lose power.



Alternate link added

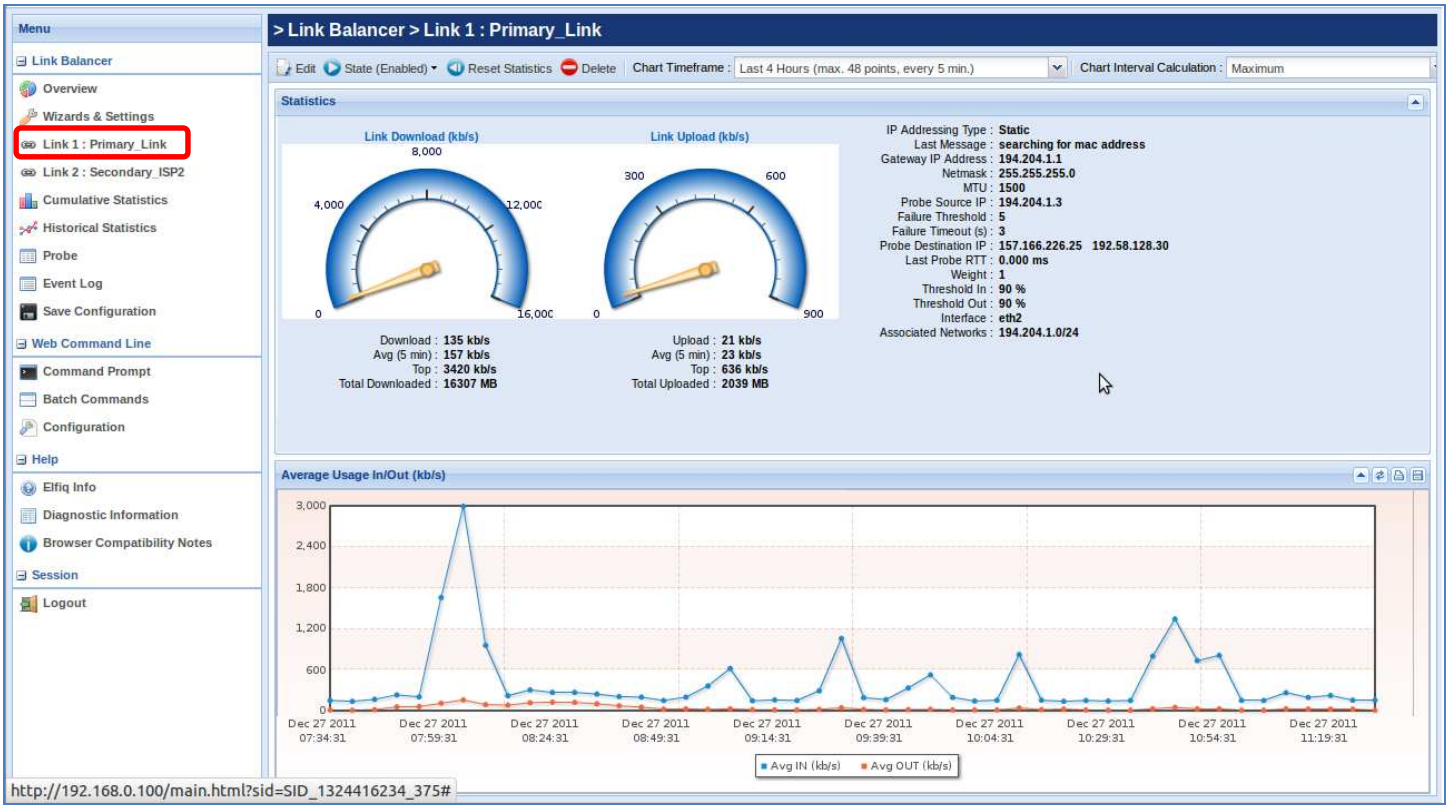
NOTE: If other devices are installed in parallel with the firewall (another independent firewall, a VPN device, relay, etc.) to the inside interface of the Link LB using a switch, additional ARP and/or ACL ARP and/or ACL NAT OUT statements could be required.

IMPORTANT: Any additional modification to the configuration after doing the step-by-step procedure requires to save the configuration in flash using the SAVE Configuration icon on the menu.

7. Verification

Once the configuration of the Link LB unit is completed, you can verify the status and usage of your links, by selecting **"Overview"**, in the left hand menu.

You can also look at each link in detail by selecting the relevant entry in the left menu.



The **"Probe"** menu option is also a useful feature that can be used to help you identify the traffic flows and adjust the algorithms in the "Outgoing load balancing" wizard (ACLNAT in rules).

The "Current Session Report"displays all current sessions.

The "Current Session Statistics" shows sessions grouped by inside IP addresses and outside addresses.

The "Cumulative Session Statistics" shows the total bandwidth per protocol, and destination ports, of all your live sessions.

The "Reset probe counters"reset all session's statistics.

Note: Event log is a good place to look for help if you have issues with your connections.