# Solution M4: Network. Software. Services (openSUSE)

There are many options and combinations to solve the tasks.

A picture containing chart

Description automatically generated

This solution is based on two **openSUSE** (using **wicked**) machines – one with two NICs, acting as server/router and a second one with one NIC, acting as client.

*Both machines are imported from templates and the MAC addresses of their network adapters are reinitialized*.

### Machine #1 – Rila

One mandatory preliminary step – set the right host name:

lsauser@vbox:~> **sudo hostnamectl set-hostname rila.lsa.lab**

Then make sure that it won’t get changed by DHCP by editing the following file:

lsauser@vbox:~> **sudo vi /etc/sysconfig/network/dhcp**

Make sure the following line (around row 214) looks like this:

**DHCLIENT\_SET\_HOSTNAME="no"**

Last but not least, we must remove all persistent MAC addresses by deleting the following:

lsauser@vbox:~> **sudo rm /etc/udev/rules.d/70-persistent-net.rules**

And finally, reboot the machine:

lsauser@vbox:~> **sudo reboot**

Once back in, we can continue.

The remaining steps could vary. Here you can see one possible and working combination.

Get information about connections

lsauser@rila:~> **ip a**

...

2: **eth0**: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000

link/ether 08:00:27:6a:41:0b brd ff:ff:ff:ff:ff:ff

altname enp0s3

inet **10.0.2.15/24** brd 10.0.2.255 scope global eth0

...

3: **eth1**: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000

link/ether 08:00:27:a4:2c:08 brd ff:ff:ff:ff:ff:ff

altname enp0s8

lsauser@rila:~>

And configure the second adapter with static IP address by creating a new file:

lsauser@rila:~> **sudo vi /etc/sysconfig/network/ifcfg-eth1**

With the following content:

**BOOTPROTO='static'**

**IPADDR='192.168.148.1/24'**

**STARTMODE='auto'**

**DHCLIENT\_SET\_DEFAULT\_ROUTE='no'**

Save and close the file.

Now apply the configuration *(the following assumes that the interface in question is DOWN):*

lsauser@rila:~> **sudo systemctl restart network**

And check the resulting configuration:

lsauser@rila:~> **ip a s eth1**

3: **eth1**: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000

link/ether 08:00:27:a4:2c:08 brd ff:ff:ff:ff:ff:ff

altname enp0s8

inet **192.168.148.1/24** brd 192.168.148.255 scope global eth1

valid\_lft forever preferred\_lft forever

inet6 fe80::a00:27ff:fea4:2c08/64 scope link

valid\_lft forever preferred\_lft forever

lsauser@rila:~>

Install the **DHCP** service:

lsauser@rila:~> **sudo zypper install -y dhcp-server**

...

First, configure the interface that we are about to use. Open the respective file for editing:

lsauser@rila:~$ **sudo nano /etc/default/isc-dhcp-server**

And make sure that the last two lines look like this (adjust the name of the adapter to match your case):

lsauser@rila:~> **sudo vi /etc/sysconfig/dhcpd**

...

# Examples: DHCPD\_INTERFACE="eth0 eth1 eth2"

# DHCPD\_INTERFACE="ANY"

#

**DHCPD\_INTERFACE="eth1"**

...

Save and close the file.

Then, open the main configuration file for editing:

lsauser@rila:~> **sudo vi /etc/dhcpd.conf**

And make sure that it has the following block (it will be best to remove everything and enter the lines below):

**option domain-name "lsa.lab";**

**option domain-name-servers 8.8.8.8;**

**default-lease-time 600;**

**max-lease-time 7200;**

**subnet 192.168.148.0 netmask 255.255.255.0 {**

**range 192.168.148.50 192.168.148.59;**

**option routers 192.168.148.1;**

**option broadcast-address 192.168.148.255;**

**}**

Then test the configuration with:

lsauser@rila:~> **sudo dhcpd -t**

Internet Systems Consortium DHCP Server 4.3.6-P1

Copyright 2004-2018 Internet Systems Consortium.

All rights reserved.

For info, please visit https://www.isc.org/software/dhcp/

Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not specified in the config file

Config file: /etc/dhcpd.conf

Database file: /var/lib/dhcp/db/dhcpd.leases

PID file: /var/run/dhcpd.pid

With this the process of base DHCP configuration is over. We must start and enable the service:

lsauser@rila:~> **sudo systemctl start dhcpd**

lsauser@rila:~> **sudo systemctl enable dhcpd**

Created symlink /etc/systemd/system/dhcp-server.service → /usr/lib/systemd/system/dhcpd.service.

Created symlink /etc/systemd/system/multi-user.target.wants/dhcpd.service → /usr/lib/systemd/system/dhcpd.service.

lsauser@rila:~> **systemctl status dhcpd**

● dhcpd.service - ISC DHCPv4 Server

Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)

Active: active (running) since Fri 2024-10-04 19:22:09 EEST; 16s ago

Main PID: 15381 (dhcpd)

Tasks: 1 (limit: 2323)

CGroup: /system.slice/dhcpd.service

└─ 15381 /usr/sbin/dhcpd -4 -cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid -chroot /var/lib/dhcp -lf /db/dhcpd>

lsauser@rila:~>

All should be “green” and the service should be running without any errors.

**SSH** is usually installed during the installation process of **openSUSE**. We can check if indeed it is there and running:

lsauser@rila:~> **systemctl** status sshd

● sshd.service - OpenSSH Daemon

Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)

Active: active (running) since Fri 2024-10-04 19:10:45 EEST; 13min ago

Main PID: 1349 (sshd)

Tasks: 1

CGroup: /system.slice/sshd.service

└─ 1349 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

lsauser@rila:~>

*If we do not see something like this, then we must install it and start it (we should know by now how to do it).*

Check the status of the firewall:

lsauser@rila:~> **systemctl status firewalld**

If it is stopped, start it. Then list the active zones with:

lsauser@rila:~> **sudo firewall-cmd --get-active-zones**

docker

interfaces: docker0

public

interfaces: eth0 eth1

lsauser@rila:~>

Now, let's set each interface in the appropriate zone:

lsauser@jupiter:~> **sudo firewall-cmd --zone=external --change-interface=eth0 --permanent**

success

lsauser@jupiter:~> **sudo firewall-cmd --zone=internal --change-interface=eth1 --permanent**

success

lsauser@jupiter:~> **sudo firewall-cmd --reload**

success

lsauser@jupiter:~> **sudo firewall-cmd --get-active-zones**

external

interfaces: eth0

internal

interfaces: eth1

lsauser@jupiter:~>

*If we do not see the above, then we could help by restarting the network service:*

*lsauser@rila:~>* ***sudo systemctl restart network.service***

Check that the NAT/forwarding functionality is enabled:

lsauser@rila:~> **cat /proc/sys/net/ipv4/ip\_forward**

**1**

lsauser@rila:~>

If the above command returned **1**, we are fine.

Let’s see what services are allowed in the **external** zone:

lsauser@rila:~> **sudo firewall-cmd --list-services --zone external**

**ssh**

lsauser@rila:~>

The SSH service is usually enabled by default.

By now, we should be done with the networking part. Our client station should already have its IP address and should have access to the Internet.

Let’s continue with the rest of the steps.

Check the instructions at **repos.zahariev.pro** and register the repository. Let’s use the first option

lsauser@rila:~> **sudo zypper addrepo https://repos.zahariev.pro/zypper zahariev-repo**

Adding repository 'zahariev-repo' ................................................................................[done]

Repository 'zahariev-repo' successfully added

URI : https://repos.zahariev.pro/zypper

Enabled : Yes

GPG Check : Yes

Autorefresh : No

Priority : 99 (default priority)

Repository priorities are without effect. All enabled repositories share the same priority.

lsauser@rila:~>

Install the required package

lsauser@rila:~> **sudo zypper install hello-lsa**

Warning: File 'repomd.xml' from repository 'zahariev-repo' is unsigned.

Note: Signing data enables the recipient to verify that no modifications occurred after the data

were signed. Accepting data with no, wrong or unknown signature can lead to a corrupted system

and in extreme cases even to a system compromise.

Note: File 'repomd.xml' is the repositories master index file. It ensures the integrity of the

whole repo.

Warning: We can't verify that no one meddled with this file, so it might not be trustworthy

anymore! You should not continue unless you know it's safe.

File 'repomd.xml' from repository 'zahariev-repo' is unsigned.

Continue? [yes/no] (no): **yes**

Building repository 'zahariev-repo' cache ........................................................................[done]

Loading repository data...

Reading installed packages...

Resolving package dependencies...

The following NEW package is going to be installed:

hello-lsa

1 new package to install.

Overall download size: 10.6 KiB. Already cached: 0 B. After the operation, additional 8.2 KiB will be used.

Backend: classic\_rpmtrans

Continue? [y/n/v/...? shows all options] (y): **y**

Retrieving: hello-lsa-1.0-1.el8.x86\_64 (zahariev-repo) (1/1), 10.6 KiB

Retrieving: hello-lsa-1.0-1.el8.x86\_64.rpm .......................................................................[done]

hello-lsa-1.0-1.el8.x86\_64.rpm:

Package header is not signed!

hello-lsa-1.0-1.el8.x86\_64 (zahariev-repo): Signature verification failed [6-File is unsigned]

Abort, retry, ignore? [a/r/i] (a): **i**

Checking for file conflicts: .....................................................................................[done]

(1/1) Installing: hello-lsa-1.0-1.el8.x86\_64 .....................................................................[done]

lsauser@rila:~>

Check that the package is installed and working

lsauser@rila:~> **hello-lsa**

\_ \_ \_ \_ \_ \_\_\_\_ \_

| | | | \_\_\_| | | \_\_\_ | | / \_\_\_| / \

| |\_| |/ \_ \ | |/ \_ \ | | \\_\_\_ \ / \_ \

| \_ | \_\_/ | | (\_) | | |\_\_\_ \_\_\_) / \_\_\_ \

|\_| |\_|\\_\_\_|\_|\_|\\_\_\_/ |\_\_\_\_\_|\_\_\_\_/\_/ \\_\

lsauser@rila:~>

That is, it. We are done here.

### Machine #2 – Pirin

One mandatory preliminary step – set the right host name:

lsauser@vbox:~> **sudo hostnamectl set-hostname pirin.lsa.lab**

Then make sure that it won’t get changed by DHCP by editing the following file:

lsauser@vbox:~> **sudo vi /etc/sysconfig/network/dhcp**

Make sure the following line (around row 214) looks like this:

**DHCLIENT\_SET\_HOSTNAME="no"**

Last but not least, we must remove all persistent MAC addresses by deleting the following:

lsauser@vbox:~> **sudo rm /etc/udev/rules.d/70-persistent-net.rules**

And finally, reboot the machine:

lsauser@vbox:~> **sudo reboot**

Once back in, we can continue.

By default, the network is set up to acquire IP address via **DHCP**.

If we check, now we will see that there is an address acquired via **DHCP**:

lsauser@pirin:~> **ip a**

...

inet **192.168.148.50/24**

...

Let’s test that we can reach resources on the local network and Internet

lsauser@pirin:~> **ping -c 4 192.168.148.1**

...

lsauser@pirin:~> **ping -c 4 8.8.8.8**

...

Create a new user with the required attributes

lsauser@pirin:~> **sudo useradd -m -c 'Homework User' homework**

...

Set the requested password

lsauser@pirin:~> **sudo passwd homework**

...

Finally, make it part of the **sudoers** users.

First, before anything else, let’s add our user to the **wheel** group:

lsauser@pirin:~> **sudo usermod -aG wheel lsauser**

Now, open the file for editing:

lsauser@pirin:~> **sudo visudo**

Then, comment lines 69 and 70 (approximately):

**# Defaults targetpw**

**# ALL ALL=(ALL) ALL**

Finally, check if the **wheel** group is active and if not activate it by uncommenting the line (approx. 82)

**%wheel ALL=(ALL:ALL) ALL**

Save and close the file. Don’t forget to close and reopen the session

*Now, note that the next time you use* ***sudo****, you will be asked to enter* ***your password*** *instead of the* ***root’s password****.*

And then make it a member of the **wheel** group

lsauser@pirin:~> **sudo usermod -aG wheel homework**

We are done with this.

**SSH** is usually installed during the installation process of **openSUSE**.

Then, we must change the default configuration and switch to port **50022**

lsauser@pirin:~> **sudo vi /etc/ssh/sshd\_config**

...

**Port 50022**

...

Once done, we must restart the service and check its status

lsauser@pirin:~> **sudo systemctl restart sshd**

lsauser@pirin:~> **systemctl status sshd**

...

Modify the firewall configuration

lsauser@pirin:~> **sudo firewall-cmd --add-port 50022/tcp --permanent**

lsauser@pirin:~> **sudo firewall-cmd --reload**

That is, it. We are done here as well.