# Solution M4: Network. Software. Services

There are many options and combinations to solve the tasks. This solution is based on one **Ubuntu** machine (with two NICs) and one **openSUSE** machine (with one NIC).

Internal virtual network will be named **NET1** and both the second network adapter of the **Ubuntu** machine and the only network adapter of the **openSUSE** machine will be connected to it.

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

### Machine #1 – Rila (Ubuntu)

One preliminary step – set the right host name, set it to preserve the name, and reboot the machine:

lsauser@ubuntu:~$ **sudo hostnamectl set-hostname rila.sulab.local**

lsauser@ubuntu:~$ **sudo vi /etc/cloud/cloud.cfg**

...

**preserve\_hostname: true**

...

lsauser@ubuntu:~$ **sudo reboot**

Other steps could be:

1. Get information about connections and configure the second adapter with static IP address:

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

**...**

lsauser@rila:~$ **sudo vi /etc/netplan/50-cloud-init.yaml**

**...**

**network:**

**ethernets:**

**enp0s3:**

**dhcp4: true**

**enp0s8:**

**addresses: [192.168.135.1/24]**

**dhcp4: no**

**version: 2**

**...**

lsauser@rila:~$ **sudo netplan apply --debug**

lsauser@rila:~$ **sudo netplan apply**

lsauser@rila:~$ **ip a s enp0s8**

**3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000**

**link/ether 08:00:27:d9:c1:a6 brd ff:ff:ff:ff:ff:ff**

**inet 192.168.135.1/24 brd 192.168.135.255 scope global enp0s8**

**valid\_lft forever preferred\_lft forever**

**inet6 fe80::a00:27ff:fed9:c1a6/64 scope link**

**valid\_lft forever preferred\_lft forever**

lsauser@rila:~$

1. Install and configure the DHCP service:

lsauser@rila:~$ **sudo apt-get install -y isc-dhcp-server**

...

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

**...**

**option domain-name "sulab.local";**

**option domain-name-servers 192.168.80.1, 8.8.8.8;**

**default-lease-time 600;**

**max-lease-time 7200;**

**subnet 192.168.135.0 netmask 255.255.255.0 {**

**range 192.168.135.50 192.168.135.99;**

**option routers 192.168.135.1;**

**option broadcast-address 192.168.135.255;**

**}**

**...**

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

Internet Systems Consortium DHCP Server 4.4.1

Copyright 2004-2018 Internet Systems Consortium.

All rights reserved.

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

Config file: /etc/dhcp/dhcpd.conf

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

PID file: /var/run/dhcpd.pid

lsauser@rila:~$ **sudo systemctl restart isc-dhcp-server**

lsauser@rila:~$ **systemctl status isc-dhcp-server**

...

1. SSH is installed during the installation process of this Ubuntu template. If not, we can do it with:

lsauser@rila:~$ **sudo apt-get install openssh-server**

...

lsauser@rila:~$ **systemctl status ssh**

...

1. Firewall configuration:

lsauser@rila:~$ **sudo ufw status**

Status: inactive

lsauser@rila:~$ **sudo ufw enable**

...

lsauser@rila:~$ **sudo ufw status**

Status: active

lsauser@rila:~$ **sudo vi /etc/default/ufw**

...

**DEFAULT\_FORWARD\_POLICY="ACCEPT"**

...

lsauser@rila:~$ **sudo vi /etc/ufw/sysctl.conf**

...

**net/ipv4/ip\_forward=1**

...

lsauser@rila:~$ **sudo vi /etc/ufw/before.rules**

...

**# NAT table rules**

**\*nat**

**:POSTROUTING ACCEPT [0:0]**

**#**

**# Forward traffic from enp0s8 (internal) through enp0s3 (external).**

**-A POSTROUTING -s 192.168.135.0/24 -o enp0s3 -j MASQUERADE**

**# Don't delete the 'COMMIT' line or these NAT table rules won't be processed**

**COMMIT**

...

lsauser@rila:~$ **sudo ufw allow 22/tcp**

lsauser@rila:~$ **sudo ufw allow proto tcp from 192.168.135.0/24 to any**

lsauser@rila:~$ **sudo ufw disable && sudo ufw enable**

...

1. NAT – it will be automatically enabled after doing above steps. Here we just check:

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

1

lsauser@rila:~$

### Machine #2 – Pirin (openSUSE)

One preliminary step – set the right host name, set it to preserve the name, and reboot the machine:

lsauser@opensuse:~> **sudo hostnamectl set-hostname pirin.sulab.local**

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

Other steps could be:

1. By default, the network is set up to acquire IP address via DHCP but when using **wicked** as network management software and re-initialized the MAC address during the import process, we must take some additional corrective actions:

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

**...**

lsauser@pirin:~> **ls -al /etc/sysconfig/network/ifcfg-eth0**

...

lsauser@pirin:~> **sudo mv /etc/sysconfig/network/ifcfg-eth0 /etc/sysconfig/network/ifcfg-eth1**

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

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

...

inet 192.168.135.50/24

...

lsauser@pirin:~> **ping -c 4 192.168.135.1**

...

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

...

1. Install FTP server

lsauser@pirin:~> **sudo zypper install -y vsftpd**

...

lsauser@pirin:~> **sudo vi /etc/vsftpd.conf**

...

**write\_enable=YES**

...

**anonymous\_enable=NO**

...

**listen=YES**

...

**listen\_ipv6=NO**

...

lsauser@pirin:~> **sudo systemctl enable --now vsftpd**

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

...

1. Install SSH – by default it is installed and running. If it was not, we can install it with:

lsauser@pirin:~> **sudo zypper install -y openssh**

...

lsauser@pirin:~> **sudo systemctl enable --now sshd**

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

...

1. Firewall configuration

lsauser@pirin:~> **sudo firewall-cmd --add-service ftp --permanent**

lsauser@pirin:~> **sudo firewall-cmd --add-service ssh --permanent**

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

1. Internet access – because of the enabled NAT-ing we can access Internet:

lsauser@pirin:~> **ping -c 4 distrowatch.com**