Guide: Linux Router (Kea + BIND)

Prerequisites

- **Log in as root:** sudo -i
- **Editor:** nano or vi

1. Network Configuration (Linux)

Replace X with your PC number.

WAN Interface (eth0)

```
nmcli con mod eth0 ipv4.addresses 192.168.60.200+X/24
nmcli con mod eth0 ipv4.gateway 192.168.60.254
nmcli con mod eth0 ipv4.dns "192.168.50.165 192.168.50.166"
nmcli con mod eth0 ipv4.method manual
nmcli con up eth0
```

LAN Interface (eth1)

```
nmcli con mod eth1 ipv4.addresses 192.168.11.1/24
nmcli con mod eth1 ipv4.method manual
nmcli con up eth1
```

System Setup

```
useradd username
passwd username
hostnamectl set-hostname mail.mojesluzba.cz
```

2. Windows Client Setup

- **IP Address:** 192.168.11.2
- **Subnet Mask:** 255.255.255.0
- **Gateway:** 192.168.11.1
- **DNS:** 192.168.11.1 *(Pointing to our Linux BIND server)*

3. Routing & NAT

Enable IP Forwarding

```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/ip_forward.conf
sysctl -p /etc/sysctl.d/ip_forward.conf
```

Enable NAT (Masquerade)

```
firewall-cmd --zone=public --add-masquerade --permanent
firewall-cmd --reload
```

Test: Ping 8.8.8.8 from Windows.

4. BIND (DNS Server)

Install

```
dnf install bind bind-utils -y
```

Configure /etc/named.conf Edit the options { ... }; block. Make sure it looks like this:

```
options {
    listen-on port 53 { 127.0.0.1; 192.168.11.1; };
    directory       "/var/named";
    allow-query     { localhost; 192.168.11.0/24; };
    forwarders      { 192.168.50.165; };
    recursion yes;
    dnssec-validation no;
};
```

Start Service

```
systemctl enable --now named
firewall-cmd --permanent --add-service=dns
firewall-cmd --reload
```

5. Kea (DHCP Server)

Install

```
dnf install kea -y
```

Configure /etc/kea/kea-dhcp4.conf Delete everything in the file and paste this exact JSON:

```
{
"Dhcp4": {
    "interfaces-config": {
        "interfaces": [ "eth1" ]
    },
    "lease-database": {
        "type": "memfile",
        "lfc-interval": 3600
    },
    "subnet4": [
        {
            "subnet": "192.168.11.0/24",
            "pools": [ { "pool": "192.168.11.10 - 192.168.11.100" } ],
            "option-data": [
                {
                    "name": "routers",
                    "data": "192.168.11.1"
                },
                {
                    "name": "domain-name-servers",
```

```
                    "data": "192.168.11.1"
                }
            ]
        }
    ]
}
}
```

Start Service

```
systemctl enable --now kea-dhcp4
firewall-cmd --permanent --add-service=dhcp
firewall-cmd --reload
```

6. SMTP (Postfix)

Install

```
dnf install postfix mailx -y
```

Configure /etc/postfix/main.cf Find and edit these lines:

```
myhostname = mail.mojesluzba.cz
mydomain = mojesluzba.cz
myorigin = $mydomain
inet_interfaces = all
mynetworks = 127.0.0.0/8, 192.168.11.0/24
home_mailbox = Maildir/
```

Redirect Root Mail

```
echo "root: username" >> /etc/aliases
newaliases
```

Start Service

```
systemctl enable --now postfix
firewall-cmd --permanent --add-service=smtp
firewall-cmd --reload
```

Test: echo "Test" | mail -s "Subject" root

7. HTTP (Web Server + PHP)

Install

```
dnf install httpd php -y
```

Setup Default PHP Page

```
echo "<?php phpinfo(); ?>" > /var/www/html/index.php
```

Enable UserDir (/etc/httpd/conf.d/userdir.conf)

- Comment out: #UserDir disabled
- Uncomment: UserDir public_html

Setup User Page

```
mkdir -p /home/username/public_html
echo "<h1>username Page</h1>" > /home/username/public_html/index.html
chown -R username:username /home/username/public_html
chmod 711 /home/username
```

SELinux & Start

```
setsebool -P httpd_enable_homedirs 1
systemctl enable --now httpd
firewall-cmd --permanent --add-service=http
firewall-cmd --reload
```

8. SSH Hardening

Configure /etc/ssh/sshd_config Add or modify:

```
Port 60555
AllowTcpForwarding no
AllowUsers username
```

SELinux & Firewall

```
# Allow port in SELinux
dnf install policycoreutils-python-utils -y
semanage port -a -t ssh_port_t -p tcp 60555

# Allow port in Firewall & Block default SSH
firewall-cmd --permanent --add-port=60555/tcp
firewall-cmd --permanent --remove-service=ssh
firewall-cmd --reload

# Restart SSH
systemctl restart sshd
```