LAB Journal Serie 1

Thomas Baumann & Tobias Weissert

Exercise 1 Static Routing

- Set up Git repo
- Set up LAB-Journal
- Group assingment nr: n113
- Familiarize with the virtual lab setup
- Search RHEL 7 Networking guide
- Router VM edit config of ENS4

```
Router:
Update /etc/resolve.conf
search n113.nslab.ch nslab.ch
search netlab.nslab.ch
nameserver 193.5.80.80
```

Router:

```
Update /etc/hostname
router.n113.nslab.ch
```

Router:

```
Update file: /etc/sysconfig/network-scripts/ifcfg-ens4
DEVICE=ens4
NM_CONTROLLED=no
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=none
IPADDR=193.5.80.113
PREFIX=27
GATEWAY=193.5.80.1
IPV4_FAILURE_FATAL=yes
Name="System eth0"
```

Router:

```
Update file: /etc/sysconfig/network-scripts/ifcfg-ens3
DEVICE=ens3
NM_CONTROLLED=no
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=none
IPADDR=193.5.82.129
PREFIX=27
GATEWAY=193.5.82.1
```

```
IPV4_FAILURE_FATAL=yes
Name="System eth0"
```

Router:

```
Update /etc/sysctl.conf
Net.ipv4.ip_forward = 1

sysctl -p /etc/sysctl.conf
systemctl restart network
```

Router:

```
ping 8.8.8.8 ✓
traceroute 8.8.8.8 ✓
ping google.com ✓
```

Client:

- Set IP to manual: 193.5.82.128/27 Gateway: 193.5.82.129
- Set DNS Server to 193.5.80.80

Network capture

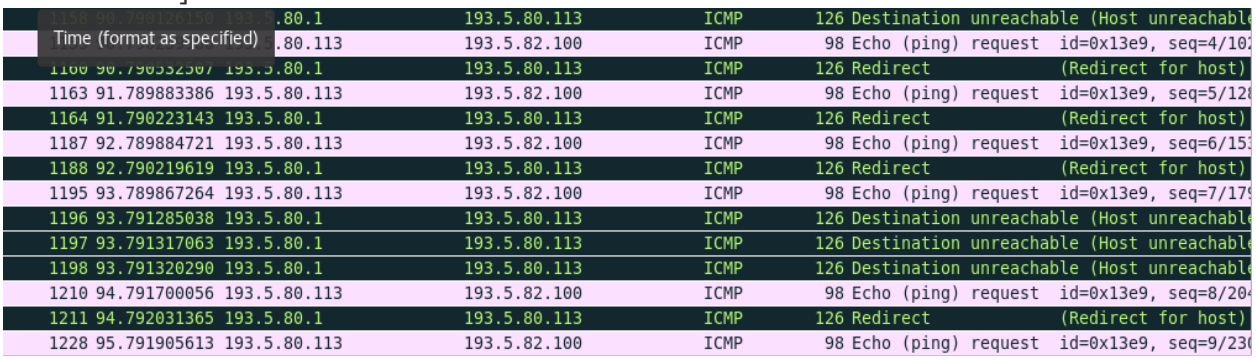
17	38.608751058	193.5.80.80	193.5.82.140	DNS	132	Standard query response 0x6ffe A 35.222.85
18	38.608953152	193.5.80.80	193.5.82.140	DNS	161	Standard query response 0xcf2f
19	39.608665694	193.5.82.140	35.222.85.5	TCP	74	37772 > http [SYN] Seq=0 Win=29200 Len=0 MS
20	39.725447352	35.222.85.5	193.5.82.140	TCP	74	http > 37772 [SYN, ACK] Seq=0 Ack=1 Win=281
21	39.725696662	193.5.82.140	35.222.85.5	TCP	66	37772 > http [ACK] Seq=1 Ack=1 Win=29312 Le
22	39.725847548	193.5.82.140	35.222.85.5	HTTP	153	GET / HTTP/1.1
23	39.840979048	35.222.85.5	193.5.82.140	TCP	66	http > 37772 [ACK] Seq=1 Ack=88 Win=29312 L
24	39.841097180	35.222.85.5	193.5.82.140	HTTP	214	HTTP/1.1 204 No Content
25	39.841118664	35.222.85.5	193.5.82.140	TCP	66	http > 37772 [FIN, ACK] Seq=149 Ack=88 Win=
26	39.841275151	193.5.82.140	35.222.85.5	TCP	66	37772 > http [ACK] Seq=88 Ack=149 Win=30336
27	39.841784699	193.5.82.140	35.222.85.5	TCP	66	37772 > http [FIN, ACK] Seq=88 Ack=150 Win=
28	39.957191683	35.222.85.5	193.5.82.140	TCP	66	http > 37772 [ACK] Seq=150 Ack=89 Win=29312
29	43.613466794	RealtekU_aa:35:4b	RealtekU_35:84:52	ARP	42	Who has 193.5.82.140? Tell 193.5.82.129
30	43.614252887	RealtekU_35:84:52	RealtekU_aa:35:4b	ARP	60	193.5.82.140 is at 52:54:00:35:84:52

ARP capture

4	3.132898275	91.189.89.199	193.5.82.140	NTP	90	NTP version 4, server
5	7.403830550	RealtekU_aa:35:4b	Broadcast	ARP	42	Who has 193.5.82.152? Tell 193.5.82.129
6	8.141342754	RealtekU_aa:35:4b	RealtekU_35:84:52	ARP	42	Who has 193.5.82.140? Tell 193.5.82.129
7	8.141726502	RealtekU_35:84:52	RealtekU_aa:35:4b	ARP	60	193.5.82.140 is at 52:54:00:35:84:52
8	8.240439588	RealtekU_35:84:52	RealtekU_aa:35:4b	ARP	60	Who has 193.5.82.129? Tell 193.5.82.140
9	8.240460242	RealtekU_aa:35:4b	RealtekU_35:84:52	ARP	42	193.5.82.129 is at 52:54:00:aa:35:4b
10	8.405454566	RealtekU_aa:35:4b	Broadcast	ARP	42	Who has 193.5.82.152? Tell 193.5.82.129
11	9.407424640	RealtekU_aa:35:4b	Broadcast	ARP	42	Who has 193.5.82.152? Tell 193.5.82.129
12	28.944359396	RealtekU_aa:35:4b	Broadcast	ARP	42	Who has 193.5.82.155? Tell 193.5.82.129
13	29.945399646	RealtekU_aa:35:4b	Broadcast	ARP	42	Who has 193.5.82.155? Tell 193.5.82.129
14	30.947404476	RealtekU_aa:35:4b	Broadcast	ARP	42	Who has 193.5.82.155? Tell 193.5.82.129
15	38.607815228	193.5.82.140	193.5.80.80	DNS	100	Standard query 0x6ffe A connectivity-check
16	38.608018932	193.5.82.140	193.5.80.80	DNS	100	Standard query 0xcf2f AAAA connectivity-ch
17	38.608751058	193.5.80.80	193.5.82.140	DNS	132	Standard query response 0x6ffe A 35.222.85

Exercise 2 Static routing – routing tables

Router: `ping 193.5.82.100 [Redirect host, nexthop: 193.5.80.112]`



Router: `ip route add 193.5.82.96/27 via 193.5.80.112 dev ens4`
Make route persistent create file /etc/sysconfig/network-scripts/route-ens4 `193.5.82.96/27 via 193.5.80.112 dev ens4`

Exercise 3 Dynamic routing – zebra service

Router: change /etc/sysconfig/network-scripts/ifcfg-ens3 and ifcfg-ens4

```
ONBOOT=no
```

Router: add to /etc/quagga/zebra.conf

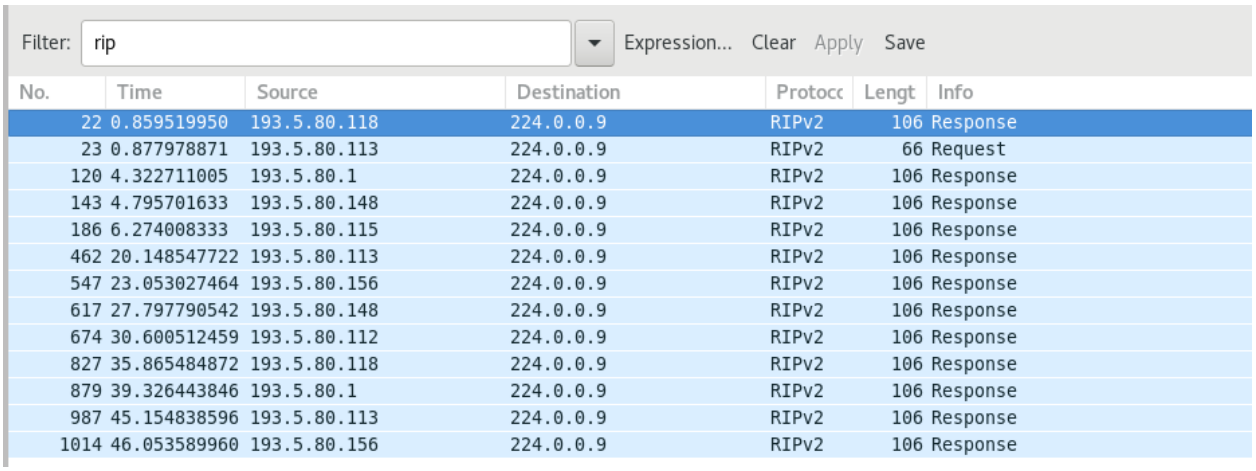
```
log file /var/log/quagga/zebra.log
systemcpl start zebra
vtysh:
conf t
interface ens3
ip address 193.5.82.129/27
interface ens4
ip address 193.80.113/27
ip route 193.5.82.96/27 193.5.80.112
ip route 193.5.82.96/27 ens4
ip route 0.0.0.0/0 193.5.80.1
write mem
vtysh:
conf t
no ip route 193.5.82.96/27 193.5.80.112
no ip route 193.5.82.96/27 ens4
no ip route 0.0.0.0/0 193.5.80.1
no ip address 193.5.82.129/27

ip address 193.5.82.129/24
ping 8.8.8.8 ✓
```

Exercise 4 Dynamic routing – RIPv2

Router: add to /etc/quagga/ripd.conf

```
log file /etc/quagga/ripd.conf
systemctl start ripd
Log contains: RIPd starting
chown quagga.quagga /var/log/qzagga/ripd.conf
vtysh
no ip route 0.0.0.0/ 193.5.80.1
conf t key chain demonet
key 1
key-string demo$rip
interface ens4
ip rip authentication mode md5
ip rip authentication key-chain demonet

router rip
redistribute connected
network 193.5.80.0/24
network ens4
distance 100 193.5.80.0/24
ping 8.8.8.8 ✓
```

```
router.n113.nslab.ch# show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface

     Network            Next Hop         Metric From            Tag Time
R(n) 0.0.0.0/0          193.5.80.1            2 193.5.80.1        0 02:34
C(i) 193.5.80.0/24      0.0.0.0               1 self              0
R(n) 193.5.82.96/27     193.5.80.112          2 193.5.80.112      0 02:46
C(r) 193.5.82.128/27    0.0.0.0               1 self (connected:1)  0
R(n) 193.5.82.160/27    193.5.80.114          2 193.5.80.114      0 02:50
R(n) 193.5.82.192/27    193.5.80.115          2 193.5.80.115      0 02:38
R(n) 193.5.83.32/27     193.5.80.118          2 193.5.80.118      0 02:44
R(n) 193.5.86.224/27    193.5.80.148          2 193.5.80.148      0 02:41
R(n) 193.5.87.224/27    193.5.80.156          2 193.5.80.156      0 02:29
router.n113.nslab.ch#
```



Filter: rip — Expression... Clear Apply Save

No.	Time	Source	Destination	Protocc	Lengt	Info
22	0.859519950	193.5.80.118	224.0.0.9	RIPv2	106	Response
23	0.877978871	193.5.80.113	224.0.0.9	RIPv2	66	Request
120	4.322711005	193.5.80.1	224.0.0.9	RIPv2	106	Response
143	4.795701633	193.5.80.148	224.0.0.9	RIPv2	106	Response
186	6.274008333	193.5.80.115	224.0.0.9	RIPv2	106	Response
462	20.148547722	193.5.80.113	224.0.0.9	RIPv2	106	Response
547	23.053027464	193.5.80.156	224.0.0.9	RIPv2	106	Response
617	27.797790542	193.5.80.148	224.0.0.9	RIPv2	106	Response
674	30.600512459	193.5.80.112	224.0.0.9	RIPv2	106	Response
827	35.865484872	193.5.80.118	224.0.0.9	RIPv2	106	Response
879	39.326443846	193.5.80.1	224.0.0.9	RIPv2	106	Response
987	45.154838596	193.5.80.113	224.0.0.9	RIPv2	106	Response
1014	46.053589960	193.5.80.156	224.0.0.9	RIPv2	106	Response

Exercise 5 Dynamic routing – OSPFv2

Router: add to /etc/quagga/ospfd.conf

```
log file /var/log/quagga/ospfd.conf
systemctl start ospfd
ospf starting
chown quagga.quagga /var/log/qzagga/ospfd.conf
vtysh coinf t
router ospf
ospf router-id 193.5.80.113
interface ens4
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 demo$ospf
redistribute connected
network 193.5.80.0/24 area 0.0.0.0
area 0.0.0.0 range 193.5.80.0/24
area 0.0.0.0 authentication message-digest
systemctl enable ospfd
```

563	21.844449628	Vmware_96:00:88	Broadcast	ARP	60 Who has 193.5.80.129? Tell 193.5.80.1
564	22.027720963	fe80::1	ff02::1:ffcd:ba52	ICMPv6	86 Neighbor Solicitation for 2001:620:500:f
565	22.060369663	193.5.82.140	151.101.114.217	TCP	66 46808 > https [ACK] Seq=1 Ack=1 Win=1136
566	22.072752411	Vmware_96:00:88	Broadcast	ARP	60 Who has 193.5.80.106? Tell 193.5.80.1
567	22.072770959	151.101.114.217	193.5.82.140	TCP	66 [TCP ACKed unseen segment] https > 46808
568	22.094426398	Vmware_96:00:88	Broadcast	ARP	60 Who has 193.5.80.93? Tell 193.5.80.1
569	22.139417442	193.5.80.118	224.0.0.251	MDNS	81 Standard query 0x0000 PTR _nmea-0183._t
570	22.159818799	Vmware_96:00:88	Broadcast	ARP	60 Who has 193.5.80.175? Tell 193.5.80.1
571	22.234665637	Vmware_96:00:88	Broadcast	ARP	60 Who has 193.5.80.121? Tell 193.5.80.1
572	22.313175881	2001:620:500:ff00::1	ff02::1	ICMPv6	86 Neighbor Advertisement 2001:620:500:ff00
573	22.365581777	Vmware_96:00:88	Broadcast	ARP	60 Who has 193.5.80.138? Tell 193.5.80.1
574	22.563145141	193.5.80.118	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
575	22.641084340	193.5.80.114	224.0.0.5	OSPF	150 Hello Packet
576	22.768826796	fe80::250:56ff:fe01:440b	ff02::5	OSPF	90 Hello Packet

Exercise 6 Dynamic routing – RIPv2 and OSPFv2

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

O   0.0.0.0/0 [110/10] via 193.5.80.1, ens4, 00:14:04
R>* 0.0.0.0/0 [100/2] via 193.5.80.1, ens4, 00:14:29
C>* 127.0.0.0/8 is directly connected, lo
O   193.5.80.0/24 [110/10] is directly connected, ens4, 00:14:05
C>* 193.5.80.0/24 is directly connected, ens4
C>* 193.5.82.128/27 is directly connected, ens3
O   193.5.82.160/27 [110/20] via 193.5.80.114, ens4, 00:12:36
R>* 193.5.82.160/27 [100/2] via 193.5.80.114, ens4, 00:13:21
O   193.5.82.192/27 [110/20] via 193.5.80.115, ens4, 00:10:48
R>* 193.5.82.192/27 [100/2] via 193.5.80.115, ens4, 00:10:57
O   193.5.83.32/27 [110/20] via 193.5.80.118, ens4, 00:10:19
R>* 193.5.83.32/27 [100/2] via 193.5.80.118, ens4, 00:10:29
O>* 193.5.85.224/27 [110/20] via 193.5.80.140, ens4, 00:14:04
O>* 193.5.86.0/27 [110/20] via 193.5.80.141, ens4, 00:14:04
O>* 193.5.86.64/27 [110/20] via 193.5.80.143, ens4, 00:14:04
O>* 193.5.86.96/27 [110/20] via 193.5.80.144, ens4, 00:14:04
O   193.5.86.224/27 [110/20] via 193.5.80.148, ens4, 00:14:04
R>* 193.5.86.224/27 [100/2] via 193.5.80.148, ens4, 00:14:29
O>* 193.5.87.128/27 [110/20] via 193.5.80.153, ens4, 00:14:04
O   193.5.87.224/27 [110/20] via 193.5.80.156, ens4, 00:14:04
R>* 193.5.87.224/27 [100/2] via 193.5.80.156, ens4, 00:14:12
```

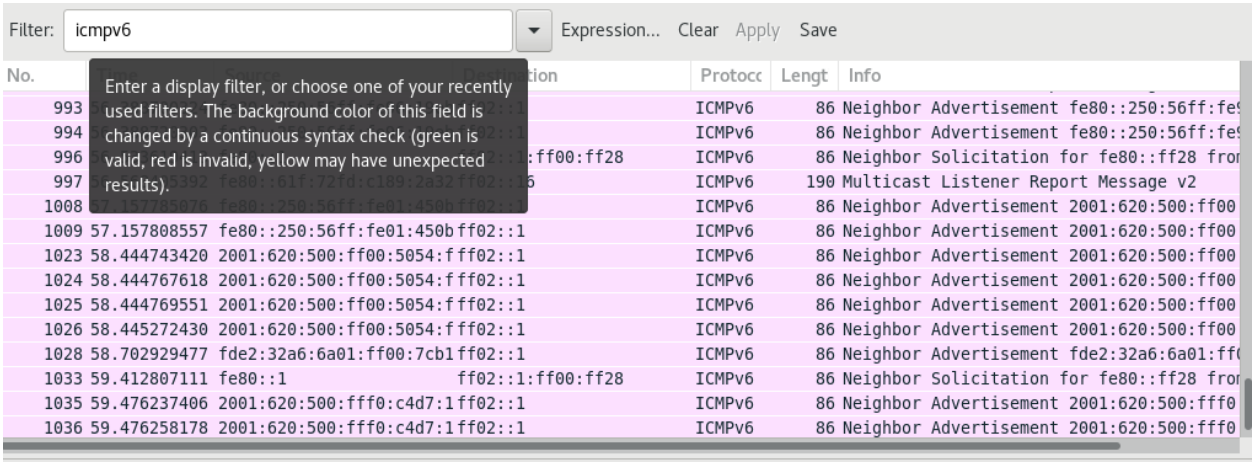
RIP has a higher priority

```
router rip
distance 120 193.5.82.160/27
ip route 192.5.80.1 0.0.0.0/0 130
```

LAB Journal Serie 2

Exercise 7 IPv6 Connectivity

```
ip -6 addr
ping6 www.switch.ch ✓
```



Source address in the router advertisment is the virtual network adapter of the VM host.

Exercise 8 IPv6 Static Routing – routing tables

```
vtysh conf t interface ens4
ipv6 address 2001:620:500:FF00::FF0D/64
ipv6 address FE80::FF0D/64

vtysh conf t interface ens3
ipv6 address 2001:620:500:FF0D::1/64
ipv6 address FE80::1/64
write mem
vtysh conf t interface ens4
ipv6 route ::/0 FE80::FC54:FF:FEE7:8557 250
write mem
ping6 switch.ch ✓
ping6 -i ens4 fe80::1 ✓
```

Exercise 9 IPv6 Router Advertisement

we prefer quagga

```
vtysh conf t interface ens3
no ipv6 ns suppress-ra
ipv6 nd prefix 2001:620:500:FF0D::/64
write mem
```

edit /etc/sysctl.conf

```
net.ipv6.conf.all.forwaring = 1
```

client

```
ip a
ipv6: 2001:620:500:FF0D:1116:6EE0:E63F:5D24/64 ✓
ping6 2001:620:FF00::FF0D ✓

ntptime
ifconfig ens3
echo e0576a5c5d45a0005054fffeaa354b | sha1sum - | cut -c31-40
vtysh interface ens3
ipv6 address fdf8:f06a:90f5::/48
ipv6 nd prefix fdf8:f06a:90f5::/48
```

Exercise 10 IPv6 dynamic routing - RIPng

edit /etc/quagga/ripngd.conf

```
log file /var/log/quagga/ospf6.conf
chown quagga.quagga /var/log/quagga/ripngd.conf
vtysh
router ripng
redistribute connected
```

Serie 3 DHCP and DNS

Exercise 12 DHCP server

edit /etc/sysconfig/network

```
NETWORKING=yes
NETWORKING_IPV6=yes
NOZEROCONF=yes
GATEWAY=193.5.82.129
IPV6_DEFAULTDEV=ens3
IPV6_DEFAULTGW=FE80::1
```

edit /etc/sysconfig/network-scripts/ifcfg-ens3

```
BOOTPROTO=static
DEVICE=ens3
ONBOOT=yes
PREFIX=27
IPADDR=193.5.82.130
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2001:620:500:FF0D::20/64
NM_CONTROLLED=no
hostnamectl set-hostname ns.n113.nslab.ch
rpm -qa | grep dhcp
```

edit /etc/dhcp/dhcpd.conf

```
option domain-name "ns113.nslab.ch";
option domain-name-servers 193.5.82.130, 193.5.80.80;

default-lease-time 300;
max-lease-time 7200;

log-facility local7;

subnet 193.5.82.128 netmask 255.255.255.224 {
  range 193.5.82.144 193.5.82.158;
  option routers 193.5.80.113;
}
systemctl start dhcpd
systemctl enable dhcpd
```

Change Client 1 from fix IP address to DHCP Client 1 got the first IP address in the range 193.5.82.144

edit /etc/dhcp/dhcpd.conf

```
host client1 {
  hardware ethernet 52:54:00:35:84:52;
  fixed-address 193.5.82.150
}
```

Client 1 got the new IP address 193.5.82.150

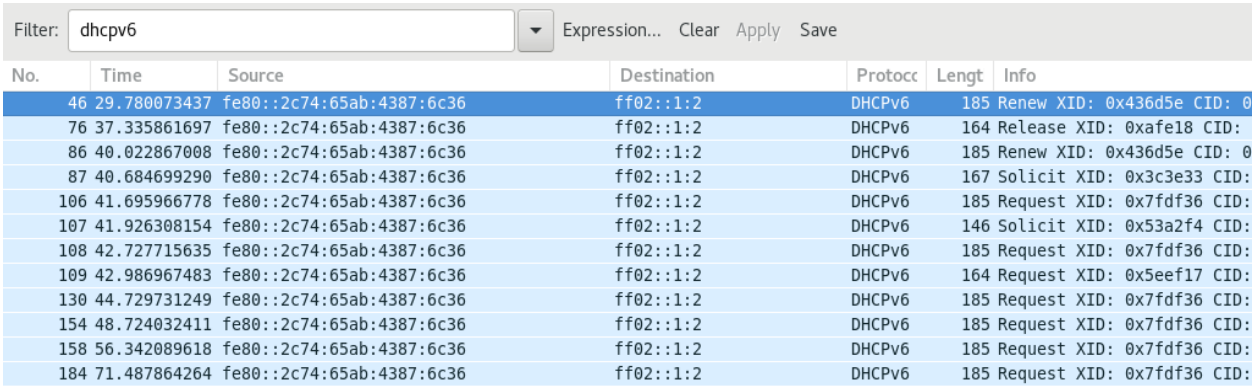
Exercise 13 DHCPv6 server

edit /etc/dhcp/dhcpd6.conf option dhcp6.name-servers 2001:620:500:ff0d::20; option dhcp6.domain-search "n113.nslab.ch";

```
subnet6 2001:620:500:ff0d::/64 {
  range6 2001:620:500:ff0d::40 2001:620:500:ff0d::2000;
}
dhcp6 start
```

client1 got a ipv6 address

```
vtysh conf interface ens3
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 nd ra-invervall 60
no ipv6 nd suppress-ra
write mem
host client1 {
  hardware ethernet 52:54:00:35:84:52;
  fixed-address6 2001:620:500:ff0d::50;
}
dhclient -6 -r
dhclient -6
```



Filter: dhcpv6 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocc	Lengt	Info
46	29.780073437	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Renew XID: 0x436d5e CID: 0
76	37.335861697	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	164	Release XID: 0xafe18 CID:
86	40.022867008	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Renew XID: 0x436d5e CID: 0
87	40.684699290	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	167	Solicit XID: 0x3c3e33 CID:
106	41.695966778	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Request XID: 0x7fdf36 CID:
107	41.926308154	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	146	Solicit XID: 0x53a2f4 CID:
108	42.727715635	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Request XID: 0x7fdf36 CID:
109	42.986967483	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	164	Request XID: 0x5eef17 CID:
130	44.729731249	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Request XID: 0x7fdf36 CID:
154	48.724032411	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Request XID: 0x7fdf36 CID:
158	56.342089618	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Request XID: 0x7fdf36 CID:
184	71.487864264	fe80::2c74:65ab:4387:6c36	ff02::1:2	DHCPv6	185	Request XID: 0x7fdf36 CID:

Exercise 14 DNS Server - Basic Configuration

Add /var/named/named.conf

```
zone "." IN{
  type hint;
  file "/var/named/named.cache";
};

zone "n113.nslab.ch" {
  type master;
  file "/var/named/fwd-n113.nslab.ch";
};
```

update fwd-n113.nslab.ch

```
;
; BIND Zone File
;
$TTL    300
@       IN      SOA     ns.n113.nslab.ch root.n113.nslab.ch (
                        2018050301      ; Serial
                        600             ; Refresh
                        300             ; Retry
                        7200            ; Expire
                        1200 )          ; Negative Cache TTL

@       IN      NS      ns
ns      IN      A       193.5.82.130
ns      IN      AAAA    2001:620:500:ff0D::20
systemctl named start
```

less var/log/messages > all zones loaded and running

add to named.conf

```
listen-on port 53 {any}
listen-on-v6 port 53 {any}
```

client01

```
dig any ns.n113.nslab.ch
```

Exercise 15 DNS Server - Zones

create file /var/named/rev-n113.nslab.ch

```
;
; BIND Zone File
;
$TTL    300
@       IN      SOA     ns.n113.nslab.ch root.n113.nslab.ch (
                        2018050301      ; Serial
                        600             ; Refresh
                        300             ; Retry
                        7200            ; Expire
                        1200 )          ; Negative Cache TTL

          IN     NS     ns.113.nslab.ch.
130       IN     PTR    ns.113.nslab.ch.
```

create file /var/named/rev6-n113.nslab.ch

```
;
; BIND Zone File
;
$TTL    300
@       IN      SOA     ns.n113.nslab.ch root.n113.nslab.ch (
                        2018050301      ; Serial
                        600             ; Refresh
                        300             ; Retry
                        7200            ; Expire
                        1200 )          ; Negative Cache TTL

;D.0        IN     NS     ns.113.nslab.ch.
;D.0        IN     PTR    ns.113.nslab.ch.
@           IN     NS     ns.113.nslab.ch.
0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN   PTR   ns.n113.nslab.ch.
```

client01

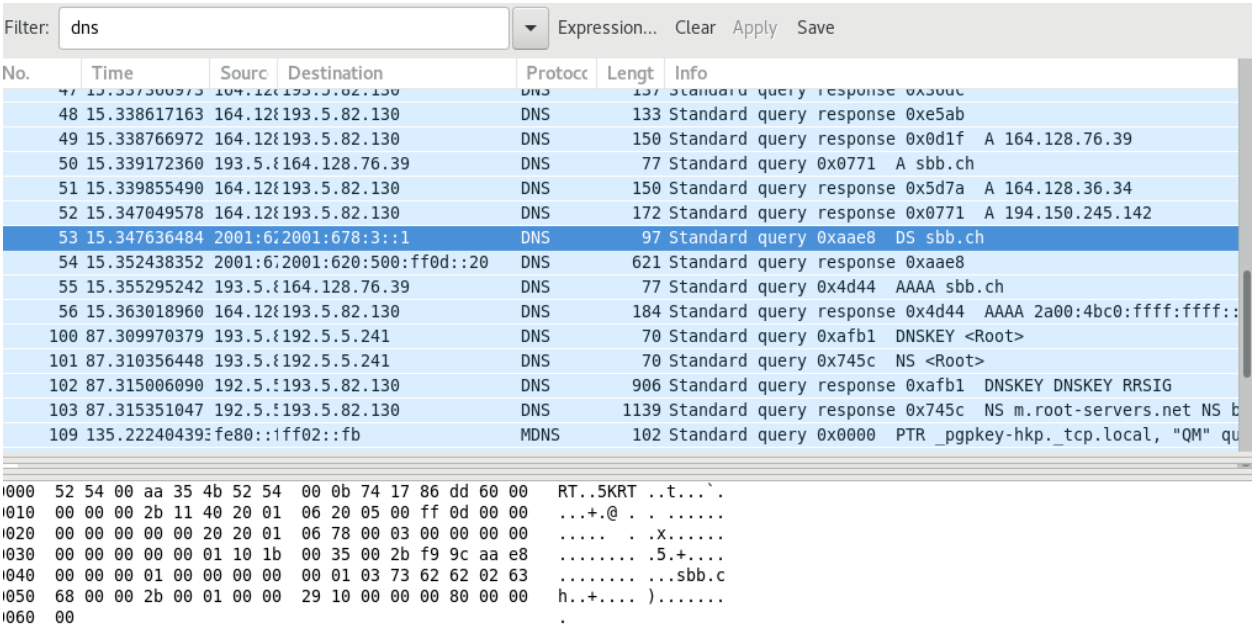
```
dig any 193.5.82.130
```

Exercise 16 DNS Server – adjust the resolver

already done earlier

Exercise 17 DNS Queries – Recordings

```
nslookup sbb.ch
```



named.conf

```
include "/etc/rndc.key";

controls {
        inet 127.0.0.1 allow { localhost; } keys { "rndc-key"; };
};
systemctl restart named
rndc status
rndc dumpdb -cache

cat /var/named/data/cache_dump.db
```

Exercise 18 DNS/DHCP – Dynamic Updates

add to /etc/dhcpd.conf

```
update-optimization false;
update-static-leases false;
```

create rndc.conf

```
server localhost {
  key  "rndc-key";
};
key "rndc-key" {
  algorithm hmac-md5;
  secret "<key>";
};
```

rndc dumpdb -
cache

```
[root@ns etc]# rndc -s localhost sync
WARNING: key file (/etc/rndc.key) exists, but using default configuration file (/etc/rndc.conf)
rndc: decode base64 secret: bad base64 encoding
[root@ns etc]# tcpdump -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
20:53:20.311527 IP 193.5.82.150.bootpc > ns.n113.nslab.ch.bootps: BOOTP/DHCP, Request from 52:54:00:35:84:52 (ou
i Unknown), length 300
20:53:20.311851 IP ns.n113.nslab.ch.bootps > 193.5.82.150.bootpc: BOOTP/DHCP, Reply, length 300
20:53:20.315650 IP ns.n113.nslab.ch.59054 > paris.netlab.bfh.ch.domain: 56297+ PTR? 130.82.5.193.in-addr.arpa. (
43)
20:53:20.320904 IP paris.netlab.bfh.ch.domain > ns.n113.nslab.ch.59054: 56297 1/5/1 PTR ns.n113.nslab.ch. (190)
20:53:20.321154 IP ns.n113.nslab.ch.34865 > paris.netlab.bfh.ch.domain: 64659+ PTR? 150.82.5.193.in-addr.arpa. (
43)
20:53:20.326282 IP paris.netlab.bfh.ch.domain > ns.n113.nslab.ch.34865: 64659 NXDomain 0/1/0 (100)
20:53:20.328114 IP ns.n113.nslab.ch.35317 > paris.netlab.bfh.ch.domain: 27320+ PTR? 2.80.87.147.in-addr.arpa. (4
2)
20:53:20.331049 IP paris.netlab.bfh.ch.domain > ns.n113.nslab.ch.35317: 27320* 1/2/4 PTR paris.netlab.bfh.ch. (1
95)
20:53:25.315611 ARP, Request who-has 193.5.82.150 tell ns.n113.nslab.ch, length 28
20:53:25.316004 ARP, Reply 193.5.82.150 is-at 52:54:00:35:84:52 (oui Unknown), length 46
20:53:25.331583 ARP, Request who-has router.n113.nslab.ch tell ns.n113.nslab.ch, length 28
20:53:25.331853 IP ns.n113.nslab.ch.48687 > paris.netlab.bfh.ch.domain: 32039+ PTR? 129.82.5.193.in-addr.arpa. (
43)
20:53:25.332067 ARP, Reply router.n113.nslab.ch is-at 52:54:00:aa:35:4b (oui Unknown), length 46
20:53:25.346257 IP paris.netlab.bfh.ch.domain > ns.n113.nslab.ch.48687: 32039 1/5/1 PTR router.n113.nslab.ch. (1
94)
20:53:25.457411 ARP, Request who-has ns.n113.nslab.ch tell 193.5.82.150, length 46
20:53:25.457429 ARP, Reply ns.n113.nslab.ch is-at 52:54:00:0b:74:17 (oui Unknown), length 28
^C
16 packets captured
```

update dhcpd.conf

```
# update dns config each time
update-optimization false;
update-static-leases true;

key DHCP_UPDATER {
 algorithm hmac-md5;
 secret Qq6gGm8yExOc7ltYRutSV47prHBMiG2Ty9okFt1zEvLmwfBGZ8UEO3VyG5uq;
};

zone n113.nslab.ch. {
  primary 193.5.82.130;
  key DHCP_UPDATER;
}

zone 128.82.5.193.in-addr.arpa. {
  primary 193.5.82.130;
  key DHCP_UPDATER;
}
```

add ipv6

```
zone D.0.F.F.0.0.5.0.0.2.6.0.1.0.0.2.ip6.arpa. {
  primary ns.113.nslab.ch;
  key DHCP_UPDATER;
}
```

Exercise 4

Exercise 19 MTA – Receiving mails

Edit etc/sysconfig/network-scripts/ifcfg-ens

```
BOOTPROTO=static
DEVICE=ens3
ONBOOT=yes
NM_CONTROLLED=no
IPADDR=193.5.82.131
NETMASK=255.255.255.224
GATEWAY=193.5.82.225
IPV6_DEFAULTDEV=ens3
IPV6_DEFAULTGW=FE80::1
IPV6ADDR=2001:620:500:FF0D::25
IPV6INIT=yes
IPV6_AUTOCONFIG=no
NETWORKING_IPV6=yes
NOZEROCONF=yes
hostnamectl set-hostname mail.n116.nslab.ch
systemctl restart network
```

Add DNS Server to Server2 Add to sysconfig/resolf.conf

```
nameserver localhost
```

Check internet connection ✅

Add DNS entry for Mail fwd-ns113.nslab.ch

```
;
; BIND Zone File
;
$ORIGIN .
$TTL    300
n113.nslab.ch   IN      SOA     ns.n113.nslab.ch. root.n113.nslab.ch. (
                                2019050301      ; Serial
                                600             ; Refresh
                                300             ; Retry
                                7200            ; Expire
                                1200 )          ; Negative Cache TTL
                NS      ns.n113.nslab.ch
                NS      root.n113.nslab.ch
;ns             IN      A       193.5.82.130
;ns             IN      AAAA    2001:620:500:FF0D::20
                IN MX 10 mail.n113.nslab.ch.
$ORIGIN n113.nslab.ch.
*                       A       193.5.83.130
                        AAAA    2001:620:500:FF0D::20

ns                      A       193.5.82.130
                        AAAA    2001:620:500:FF0D::20

server02                A       193.5.82.131
                        TXT     "00d3847fed7fe0f58ae748b59eec47c300"
mail                    A       193.5.82.131
```

Edit main.cf

```
myhostname = mail.n113.nslab.ch
mydomain = n113.nslab.ch
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
mail.n113.nslab.ch
telnet localhost 25

Trying 193.5.82.131...
Connected to mail.
Escape character is '^]'.
220 mail.n113.nslab.ch ESMTP Postfix
EHLO n113.nslab.ch
250-mail.n113.nslab.ch
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: user@n113.nslab.ch
250 2.1.0 Ok
RCPT TO: user@n113.nslab.ch
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: test
test test
.
250 2.0.0 Ok: queued as 6E4F723977E7
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Exercise 20 MTA – Sending mails

```
myhostname = mail.n113.nslab.ch
mydomain = n113.nslab.ch
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain, mail.n113.nslab.ch
```

```
[root@server02 user]# tail -f /var/log/maillog
Jun 11 19:23:54 server02 postfix/master[5310]: daemon started -- version 2.10.1, config
uration /etc/postfix
Jun 11 19:24:22 server02 postfix/smtpd[5317]: connect from localhost[::1]
Jun 11 19:24:58 server02 postfix/smtpd[5317]: 530F4302226B: client=localhost[::1]
Jun 11 19:25:03 server02 postfix/cleanup[5328]: 530F4302226B: message-id=<2019061117245
8.530F4302226B@mail.n113.nslab.ch>
Jun 11 19:25:03 server02 postfix/qmgr[5312]: 530F4302226B: from=<root@n113.nslab.ch>, s
ize=328, nrcpt=1 (queue active)
Jun 11 19:25:03 server02 postfix/local[5329]: 530F4302226B: to=<user@n113.nslab.ch>, re
lay=local, delay=13, delays=13/0.01/0/0, dsn=2.0.0, status=sent (delivered to mailbox)
Jun 11 19:25:03 server02 postfix/qmgr[5312]: 530F4302226B: removed
Jun 11 19:25:05 server02 postfix/smtpd[5317]: disconnect from localhost[::1]
Jun 14 08:43:49 server02 postfix/postfix-script[3412]: starting the Postfix mail system
Jun 14 08:43:49 server02 postfix/master[3414]: daemon started -- version 2.10.1, config
uration /etc/postfix
```

```
[user@server02 ~]$ mail
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/spool/mail/user": 2 messages 2 new
>N  1 root                  Tue Jun 11 19:22  12/424
 N  2 root@n113.nslab.ch    Tue Jun 11 19:25  13/472
&
Message  1:
From root@mail.n113.nslab.ch  Tue Jun 11 19:22:17 2019
Return-Path: <root@mail.n113.nslab.ch>
X-Original-To: user@n113.nslab.ch
Delivered-To: user@n113.nslab.ch
Date: Tue, 11 Jun 2019 19:14:28 +0200 (CEST)
From: root@mail.n113.nslab.ch (root)
Status: R

lla

&
Message  2:
From root@n113.nslab.ch  Tue Jun 11 19:25:03 2019
Return-Path: <root@n113.nslab.ch>
X-Original-To: user@n113.nslab.ch
Delivered-To: user@n113.nslab.ch
Date: Tue, 11 Jun 2019 19:24:50 +0200 (CEST)
From: root@n113.nslab.ch
Status: R
```

sudo apt install mailutils Install satelite system with n113.nslab.ch as relay

```
echo test | mail -s "das ist ein Test" thomas.baumann@students.bfh.ch
411 Message accepted for delivery)
Jun 14 10:49:08 mail postfix/qmgr[5436]: 809FE3022289: removed
Jun 14 10:49:25 mail postfix/smtpd[6247]: connect from mx1.bfh.ch[147.87.250.52]
Jun 14 10:49:25 mail postfix/smtpd[6247]: 0FB083022289: client=mx1.bfh.ch[147.87.250.52]
Jun 14 10:49:25 mail postfix/cleanup[6243]: 0FB083022289: message-id=<76625f998fb745319d58f21021710ee4@stu
dents.bfh.ch>
Jun 14 10:49:25 mail postfix/qmgr[5436]: 0FB083022289: from=<tobiashartmut.weissert@students.bfh.ch>, size
=2728, nrcpt=1 (queue active)
Jun 14 10:49:25 mail postfix/smtpd[6247]: 167EF302228B: client=mx1.bfh.ch[147.87.250.52]
Jun 14 10:49:25 mail postfix/cleanup[6243]: 167EF302228B: message-id=<5c6ade19c114431ea9c315a8c5db4b09@stu
dents.bfh.ch>
Jun 14 10:49:25 mail postfix/qmgr[5436]: 167EF302228B: from=<tobiashartmut.weissert@students.bfh.ch>, size
=2728, nrcpt=1 (queue active)
Jun 14 10:49:25 mail postfix/local[6250]: 0FB083022289: to=<user@n113.nslab.ch>, relay=local, delay=0.07,
delays=0.01/0.05/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)
Jun 14 10:49:25 mail postfix/qmgr[5436]: 0FB083022289: removed
Jun 14 10:49:26 mail postfix/local[6251]: 167EF302228B: to=<user@n113.nslab.ch>, relay=local, delay=1.1, d
elays=0.02/0.02/0/1, dsn=2.0.0, status=sent (delivered to mailbox)
Jun 14 10:49:26 mail postfix/qmgr[5436]: 167EF302228B: removed
Jun 14 10:49:27 mail postfix/smtpd[6247]: disconnect from mx1.bfh.ch[147.87.250.52]
^C
[root@mail user]# systemctl restart xinetd^C
You have new mail in /var/spool/mail/user
[root@mail user]# vi /etc/resolv.conf
[root@mail user]# mail
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/spool/mail/user": 4 messages 4 new
>N  1 root                  Tue Jun 11 19:22  12/424
 N  2 root@n113.nslab.ch    Tue Jun 11 19:25  13/472
 N  3 Weissert Tobias Hart  Fri Jun 14 10:49  68/2856  "test"
 N  4 Weissert Tobias Hart  Fri Jun 14 10:49  68/2856  "test"
```

Exercise 21 MTA – Access to mailboxes via IMAP3 (and POP3)

dovecot already installed create file /etc/dovecot/local.conf

```
systemctl start dovecot
telnet mail.n113.nslab.ch 110
```

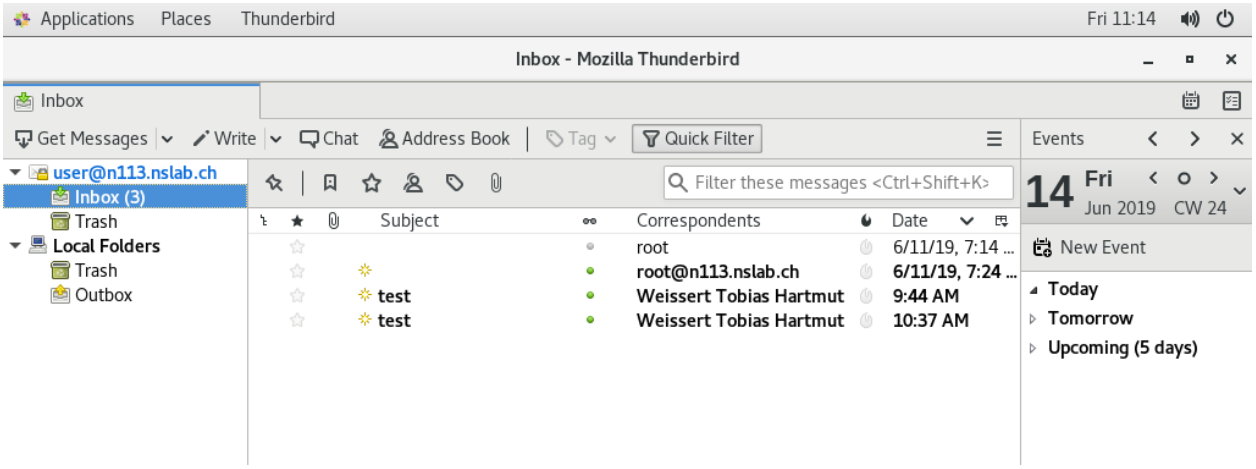
```
Jun 14 10:55:35 mail dovecot: master: Dovecot v2.2.36 (1f10bfa63) starting up for imap, pop3, lmtp (core dumps
 disabled)
^C
[root@mail user]# telnet mail.n113.nslab.ch 110
Trying 2001:620:500:ff0d::25...
Connected to mail.n113.nslab.ch.
Escape character is '^]'.
+OK Dovecot ready.
user user
+OK
lab$us3r
-ERR Unknown command.
pass lab$us3r
+OK Logged in.
stat
+OK 4 6512
retr 1
+OK 378 octets
Return-Path: <root@mail.n113.nslab.ch>
X-Original-To: user@n113.nslab.ch
Delivered-To: user@n113.nslab.ch
Received: by mail.n113.nslab.ch (Postfix, from userid 0)
        id 7C7E2302226B; Tue, 11 Jun 2019 19:14:41 +0200 (CEST)
Message-Id: <20190611171441.7C7E2302226B@mail.n113.nslab.ch>
Date: Tue, 11 Jun 2019 19:14:28 +0200 (CEST)
From: root@mail.n113.nslab.ch (root)

lla
.
```

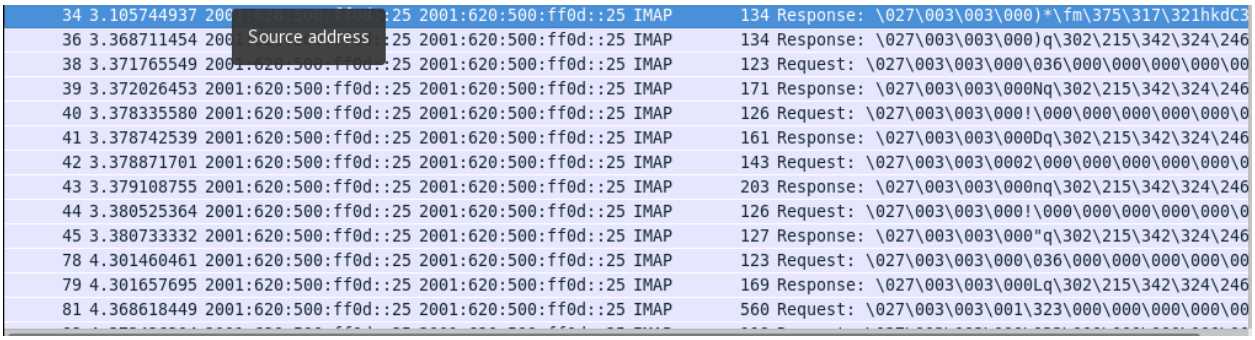
```
systemctl enable dovecot
```

edit /etc/dovecot/conf.d/10-ssl.conf

```
ssl = no
disable_plaintext_auth = no
```

Exercise 22 MTA – Configuration of a MUA





Exercise 23 Install and configure a web server with LE certificates

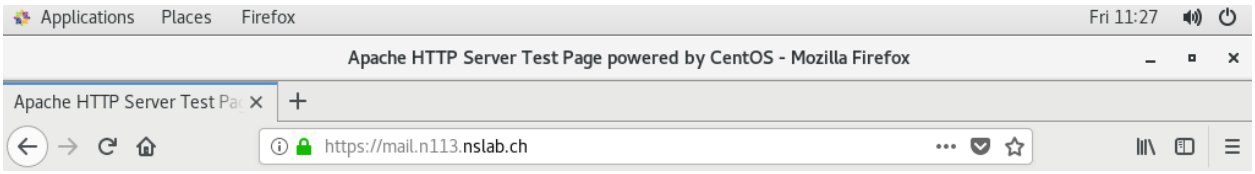
install https, php mod_ssl

create file mail.conf in /etc/https/conf.d systemctl start
httpd http://mail.n113.nslab.ch works

install certbot python2-certbot-apache

get lets encrypte certificate

https://mail.n113.nslab.ch works



edit /etc/postfix/master.cf and enable

Exercise 24 Securing the communication

systemctl enable saslauthd systemctl restart postfix

- swaks -tlso -t user@n113.nslab.ch

```
[root@mail postfix]# swaks -tlso -t user@n113.nslab.ch
=== Trying mail.n113.nslab.ch:25...
=== Connected to mail.n113.nslab.ch.
<-  220 mail.n113.nslab.ch ESMTP Postfix
 -> EHLO mail.n113.nslab.ch
<-  250-mail.n113.nslab.ch
<-  250-PIPELINING
<-  250-SIZE 10240000
```

```
<-  250-VRFY
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250 DSN
 -> STARTTLS
<-  220 2.0.0 Ready to start TLS
=== TLS started with cipher TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256
=== TLS no local certificate set
=== TLS peer DN="/CN=mail.n113.nslab.ch"
 ~> EHLO mail.n113.nslab.ch
<~  250-mail.n113.nslab.ch
<~  250-PIPELINING
<~  250-SIZE 10240000
<~  250-VRFY
<~  250-ETRN
<~  250-ENHANCEDSTATUSCODES
<~  250-8BITMIME
<~  250 DSN
 ~> MAIL FROM:<user@mail.n113.nslab.ch>
<~  250 2.1.0 Ok
 ~> RCPT TO:<user@n113.nslab.ch>
<~  250 2.1.5 Ok
 ~> DATA
<~  354 End data with <CR><LF>.<CR><LF>
 ~> Date: Fri, 14 Jun 2019 13:01:28 +0200
 ~> To: user@n113.nslab.ch
 ~> From: user@mail.n113.nslab.ch
 ~> Subject: test Fri, 14 Jun 2019 13:01:28 +0200
 ~> Message-Id: <20190614130128.005228@mail.n113.nslab.ch>
 ~> X-Mailer: swaks v20170101.0 jetmore.org/john/code/swaks/
 ~>
 ~> This is a test mailing
 ~>
 ~> .
<~  250 2.0.0 Ok: queued as 6F5DC32A9DE7
 ~> QUIT
<~  221 2.0.0 Bye
=== Connection closed with remote host.
```

- Edit /etc/dovecot/local.conf
- systemctl restart dovecot

- Test
  TLS

CheckTLS Confidence Factor for "mail.n113.nslab.ch": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
mail.n113.nslab.ch [193.5.82.131:25]	0	OK (109ms)	OK (251ms)	OK (107ms)	OK (106ms)	OK (330ms)	OK (105ms)	OK (125ms)
Average		100%	100%	100%	100%	100%	100%	100%

- To limit access to "dovecot" to
  POP3S/IMAP4

```
[root@mail user]# netstat -tulpn | grep dove
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      3312/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      3312/dovecot
tcp6       0      0 :::993                  :::*                    LISTEN      3312/dovecot
tcp6       0      0 :::995                  :::*                    LISTEN      3312/dovecot
```

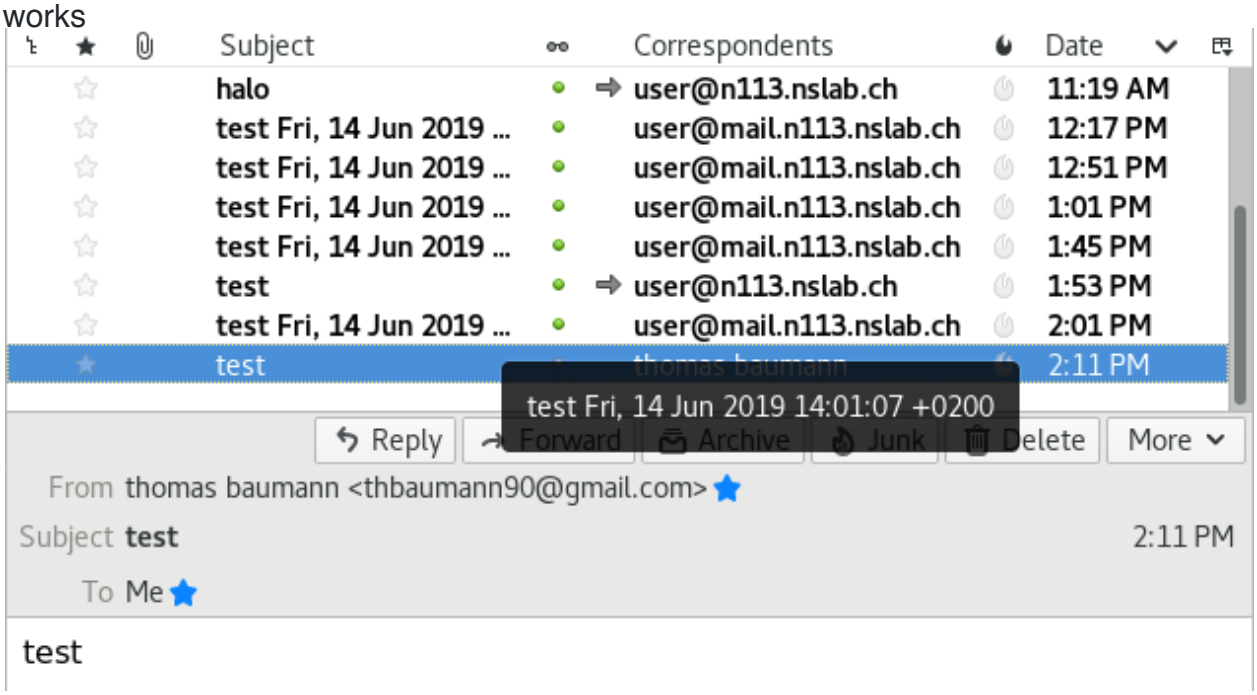
- Edit /etc/dovecot/local.conf and check log

```
Jun 14 13:49:36 mail dovecot: master: Dovecot v2.2.36 (1f10bfa63) starting up for
imap, pop3 (core dumps disabled)
```

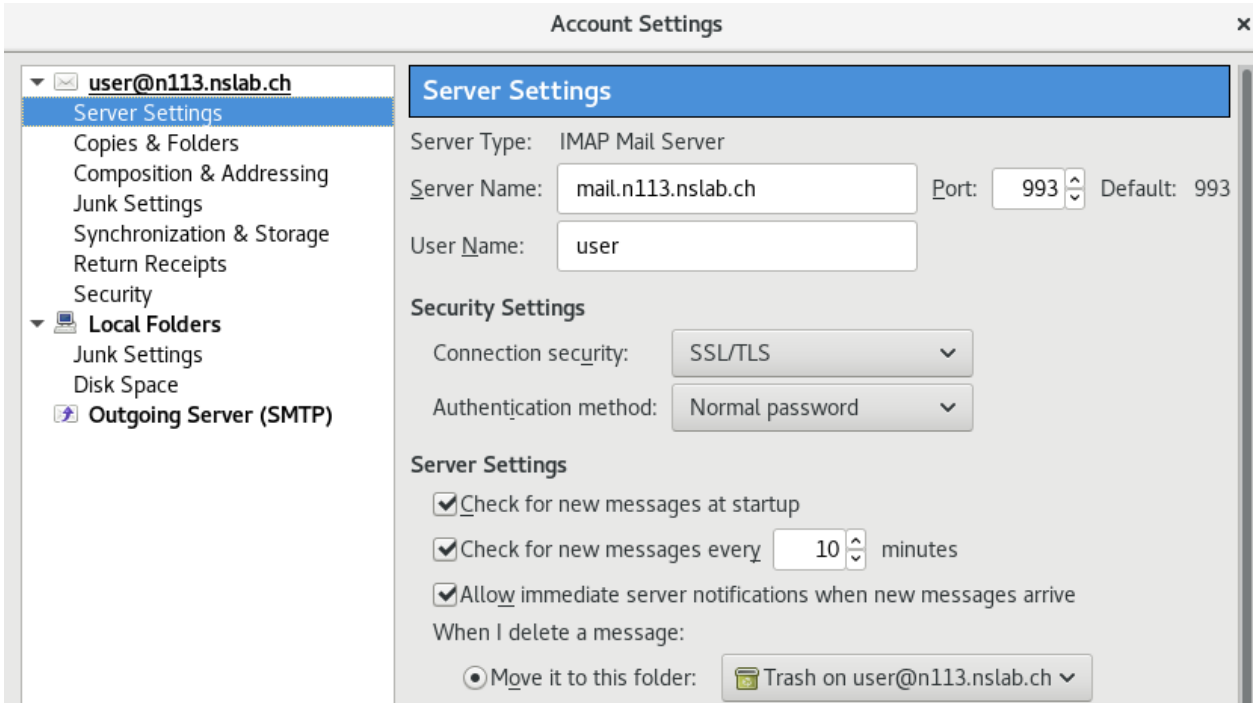
- Wireshark
  TLS

```
    26 1.551461780 2001:620:500:ff0d::25 2001:620:500:ff0d::25 SMTP      118 S: 220 2.0.0 Ready to start TLS
    27 1.559543190 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   605 Client Hello
    28 1.561005481 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2  3075 Server Hello, Certificate, Server Key Exchange,
    29 1.561035542 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TCP        88 47172 > smtp [ACK] Seq=553 Ack=3197 Win=175744 L
    30 1.561934040 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   214 Client Key Exchange, Change Cipher Spec, Encrypt
    31 1.562739762 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   314 New Session Ticket, Change Cipher Spec, Encrypte
    32 1.566171399 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   142 Application Data
    33 1.566332793 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   244 Application Data
    34 1.566550998 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   154 Application Data
    35 1.572902854 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   131 Application Data
    36 1.573052996 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   147 Application Data
    37 1.612989798 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TCP        88 smtp > 47172 [ACK] Seq=3622 Ack=858 Win=44800 Le
    38 1.632949540 2001:620:500:ff0d::25 2001:620:500:ff0d::25 TLSv1.2   131 Application Data
```

- Receive Mail works



- Config MUA

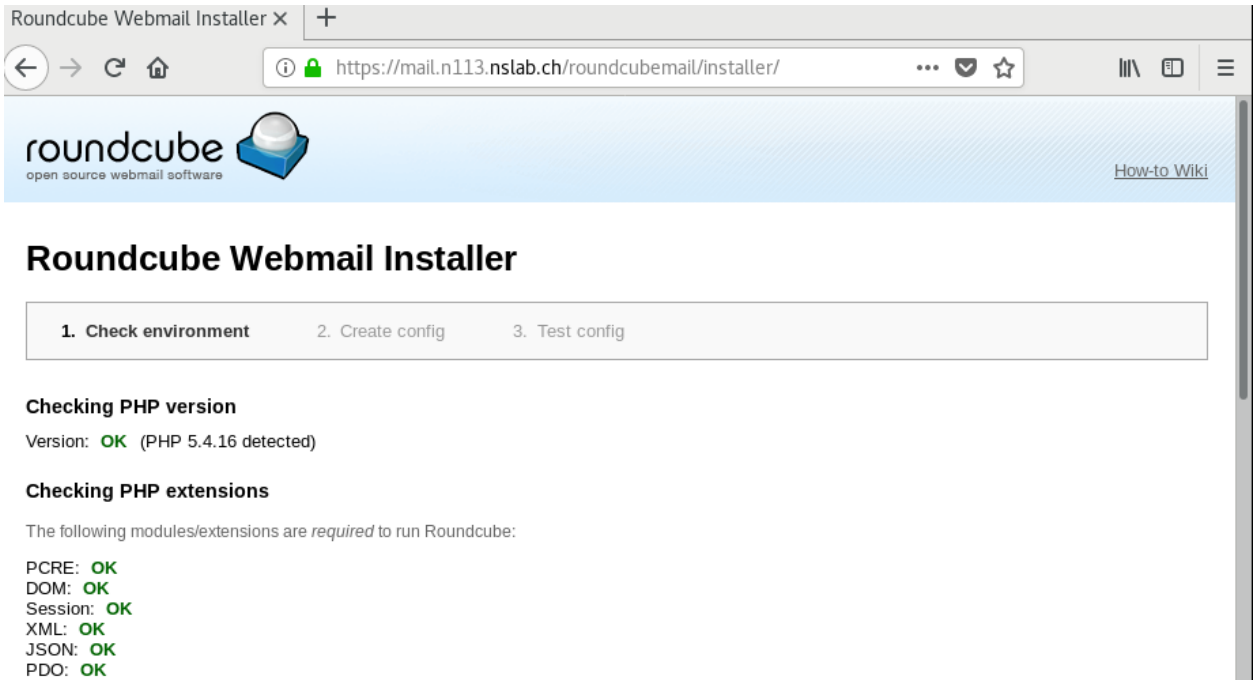


- Sending and receving Mails works!

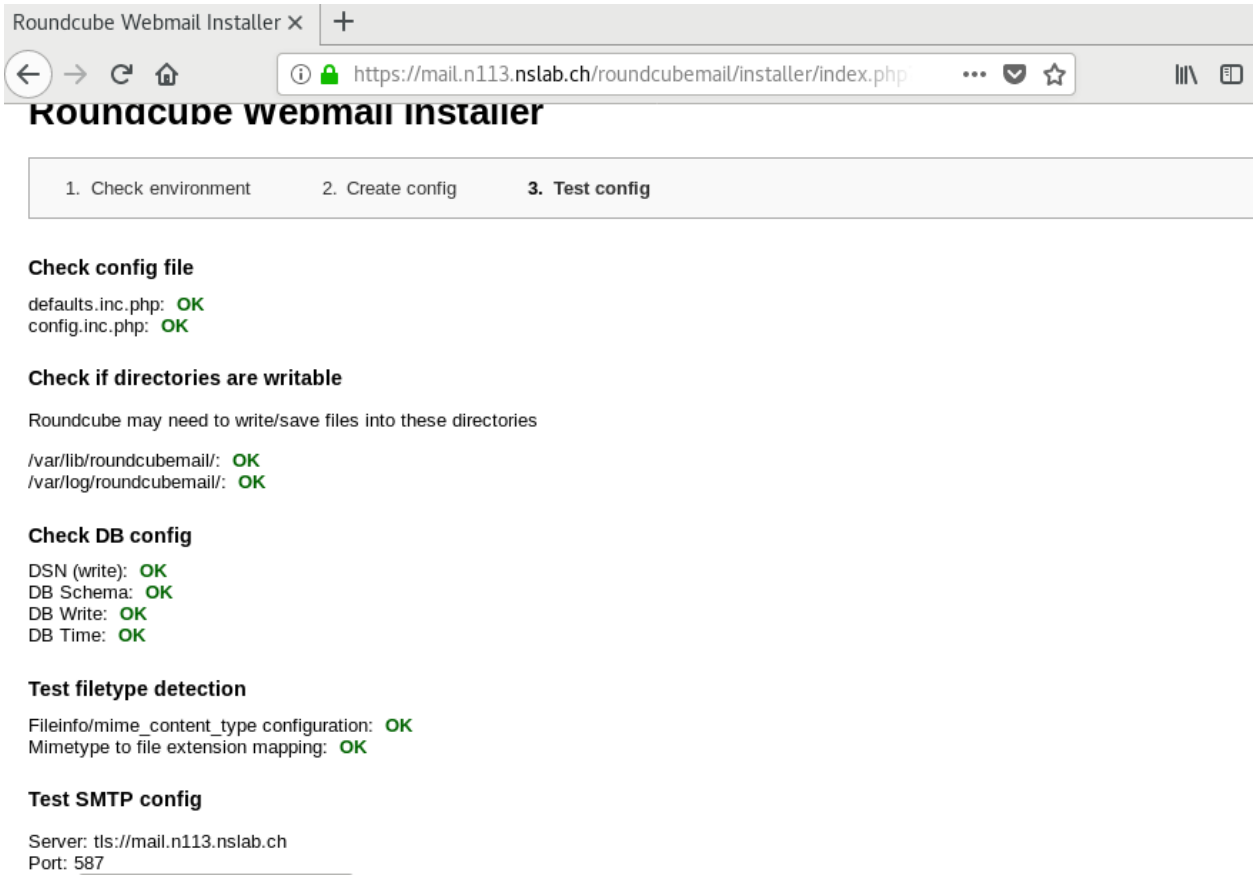
25

```
yum install --enablerepo=epel roundcubemail
```

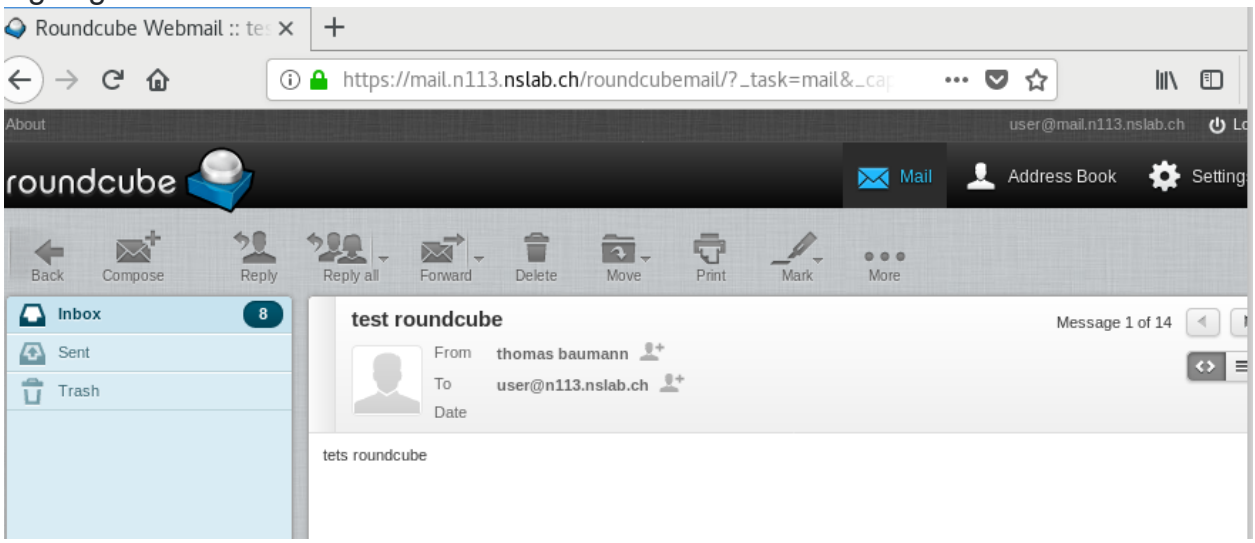
- Edit /etc/httpd/conf.d/roundcubemail.conf and verify if it works



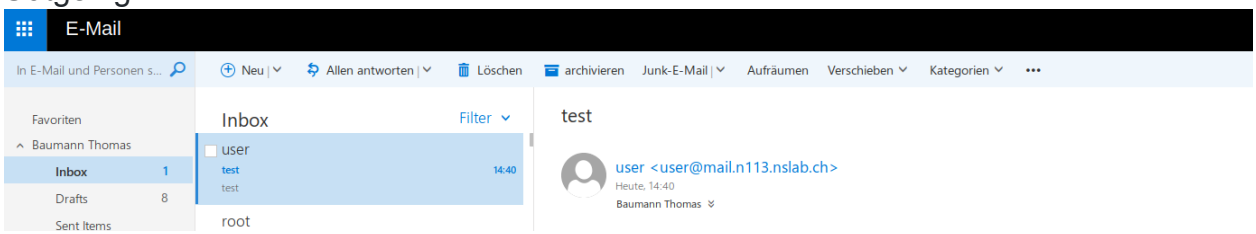
- Generate Roundcube conf and check if everything is ok:



- Login to: https://mail.n124.nslab.ch/roundcubemail/
- Test Send and receive Mails
- Ingoing



- Outgoing


E-Mail
In E-Mail und Personen s...
Neu
Allen antworten
Löschen
archivieren
Junk-E-Mail
Aufräumen
Verschieben
Kategorien
Favoriten
Baumann Thomas
Inbox 1
Drafts 8
Sent Items
Inbox
Filter
user
test
14:40
test
root
test
user <user@mail.n113.nslab.ch>
Heute, 14:40
Baumann Thomas